THE SURVEILLANCE EXPERIENCE OF CHINESE UNIVERSITY STUDENTS AND THE VALUE OF PRIVACY IN THE SURVEILLANCE SOCIETY

Chengyuan Shao

A dissertation submitted to the faculty of the University of North Carolina at Chapel Hill in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Hussman School of Journalism and Media

Chapel Hill
2020

Approved by

Tori Smith Ekstrand

Daniel Riffe

Amanda Reid

Torin Monahan

Joseph Kennedy

ABSTRACT

Shao Chengyuan: The Surveillance Experience of Chinese University Students and the Value of Privacy in the Surveillance Society
(Under the direction of Dr. Victoria Smith Ekstrand)

Against the backdrop of China's expanding surveillance infrastructure, this study focuses on the young generation internet users in China and examines their experience with government and commercial surveillance as they engage on Chinese social media and online service platforms. A nation-wide mixed-mode survey was distributed to university students in five Chinese cities. Research findings suggest that the young generation internet users in China live in a fundamental paradox where their desire to fully engage in the digital world confronts the growing concerns about mass surveillance from the increasingly powerful platforms and the traditional state power. As a result, they would make situationally contextualized privacy decisions based on the type of personal information and the platform on which the information is disclosed. They would also practice self-censorship responding to questions about privacy and surveillance in online environments. These findings have important implications for research on privacy and surveillance in China and more broadly on information policy in the surveillance age.

To my advisor, Dr. Tori Ekstrand, for opening the door to a great adventure for me and guiding my academic life with so much grace and wisdom. I truly could not have done this without you.

To my parents, Mama and Baba, for always cheering me on. I would not have the courage to go explore the world halfway across the globe without knowing that you are always there for me at home.

To my boyfriend, Hu Min, for all his love and inspiration in the past seven years. This journey would have been a lot more lonely and difficult without you in my life.

To my dear friends from Chapel Hill, you know who you are, for the fun times that we shared. Your friendship made my stay in the United States memorable.

ACKNOWLEDGEMENTS

I wish to thank the members of my dissertation committee: Dr. Daniel Riffe, Dr. Amanda Reid, Dr. Torin Monahan, and Prof. Joseph Kennedy for generously offering their time, guidance and good will throughout this project.

Special thanks to Dr. Chen Juan at South China University of Technology and Dr. Li Bing at Zhejiang University of Technology for their generous contribution to this project. I would also like to thank Dr. Lu Juan, Dr. Wang Wenjie, Dr. Liu Jinhong, Dr. Peng Guibing, Dr. Wang Lingning, and Dr. Li Yifei for their local support in obtaining the necessary documentations that helped put this project through the Institutional Review Board.

Finally, I thankfully acknowledge the China Scholarship Council for its generous support of my education at the University of North Carolina at Chapel Hill.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The rise of the surveillance society in the past two decades has called for renewed attention to theory and policy on emerging surveillance practices that have penetrated every corner of contemporary social life (Lyon, 2002, 2015; Cohen, 2008, 2003, 2015; Richards, 2013). In this surveillance society, precise details of individuals' personal lives are "collected, stored, retrieved, and processed within huge computer databases" by corporations and governments to influence and manage people and populations (Lyon, 1994, 2002). In recent years, cutting-edge artificial intelligence based on networked machine-learning systems and new wave sensor-enabled devices has magnified the capacity of governments and internet platforms around the world to collect and process massive information about individuals and groups. This development of contemporary life is creating growing challenges to dominant approaches to privacy, which were inadequate in pinpointing sources of disruption and addressing the harms caused by a burgeoning array of contemporary surveillance practices.

As traditionally understood, privacy is the right to be left alone and the right to maintain control over personal information flow (Warren & Brandeis, 1890; Westin, 2003). In a time of significant transformation in data practices enabled by information and computational technologies, these rights are frequently sacrificed when balanced against other pressing interests, such as security, efficiency, and innovation. This is so prevalent that privacy has been said to be on its way to become an anachronistic value (Rule, 2016, p.8). As the efficiency-minded governments and profit-seeking businesses of our time continue to identify connections between personal data and new ways of control and persuasion, and successfully evade

entrenched regulatory approaches while doing so, it is necessary that concepts and policies around privacy be revisited in the context of an emerging surveillance society on a global scale.

When considering the major changes initiated by new communication technologies, to borrow the words from Balkin (2014), asking what is genuinely new is to ask the wrong question; the focus ought to be on what features of the human condition a technology has made particularly salient that went relatively unnoticed before, and what consequences it will have for human freedom. Facing the new wave of privacy threats as identified above, it is simply not enough to note the ever-expanding capability of governments and private internet platforms to collect and monitor new personal data, such as location history, biological indicators, and intellectual preference. New perspectives need to be brought forward about the nature of contemporary surveillance practices and the purpose of privacy in the networked society; questions need to be asked about conventional wisdom on the binary oppositions between public and private and between authoritarianism and democracy that contemporary surveillance systems have made problematic. Only by highlighting these issues can new understandings about privacy be formed and new approaches to information policies around privacy and surveillance be properly addressed.

China, as the world's largest internet population and a long-time one-party post-authoritarian state, has been placed under the spotlight in prevailing discussions about the harm of surveillance in the digital age. Western media have reported on China's national surveillance system based on novel facial recognition technologies and a social credit system, both of which are under rapid development in recent years. This raises concerns about the possible abuse of such technologies in a non-democratic society where political dissidents have been prosecuted without due process and transparency (Mitchell & Diamond, 2018, Feb 2; Millward, 2018, Feb

3; Carney, 2018, Sept 17). One of the new developments captured in the media is that China's facial recognition technologies are now capable of detecting and labeling people's ethnicities and that such technologies are used to monitor the activities of Uyghur Muslims, a population that has been under severe state surveillance in recent years (Mozur, 2019, April 14; Doffman, 2019, May 3).

However, as Richards (2013) points out, while authoritarian regimes have long been the primary villains in stories the West tells about surveillance, such one-dimensional Orwellian portraits of surveillance fail to grasp the essence of the harm of surveillance in contemporary societies. For instance, democratically elected governments in the West have also stepped up their surveillance of the public in the name of counter-terrorism, protecting cybersecurity, and a growing list of other concerns. Government surveillance, such as the NSA wiretapping of citizen's communications and the British data-retention regulation, are some evident examples. Recent investigative pieces also found that U.S. universities, private foundations, and retirement funds have invested hundreds of millions of dollars into the facial recognition technologies behind state surveillance in China (Mac, Adams, & Rajagopalan, 2019, June 5). More importantly, the Orwellian digital dystopia account of surveillance risks losing sight of a vital component of contemporary surveillance systems—commercial surveillance for the purposes of marketing and profit making that is led by the business sector and has largely infiltrated many aspects of modern people's lives.

Currently, on the Chinese internet, more than 800 million users feed a substantial amount of personal data to powerful private platforms including but not limited to Alibaba, Tencent, and Baidu, who control the most popular online shopping, banking, mapping, and social media applications. This provides fertile soil for the expansion of commercial surveillance. In fact, with

the development of Smart City and industry transformation, China has seen accelerated growth in the use of big-data technology in different industries, including manufacturing, transportation, healthcare, retail, and e-commerce, which fuels the growth of business analytics services in recent years (The Financial, 2015). Moreover, business analytic services are increasingly cooperating with public institutions in government-related fields, thus nurturing a neoliberal form of governance and data politics in China (Hou, 2017).

Against that backdrop, the Chinese surveillance society as well as the surveillance experience of young generation internet users in China are fundamentally multi-dimensional, shaped by the combined force of a traditionally strong state surveillance system and a dynamic commercial surveillance network. Such a surveillance system transcends what, by far, has only been characterized as an Orwellian digital dystopia and calls for more nuanced treatment of surveillance power in a non-Western context. This dissertation explores this subject by investigating how both state and commercial surveillance are experienced among the young generation internet users in China and how such experience has shaped the privacy beliefs and information-sharing behaviors among this unique population. This investigation seeks to shed light on how new generation Chinese internet users perceive surveillance practices from the government and internet platforms, their concerns about state and commercial surveillance power, and how they make contextualized privacy decisions in the emerging surveillance society in China.

The population under investigation in this dissertation is university students currently enrolled in higher education institutions in China. This population is chosen because it is the most actively engaged group in contemporary Chinese information society. According to statistics from China Internet Network Information Center (CINIC, 2018), university students are

among the most active users of social media platforms, such as WeChat, QQ, and Weibo, and service platforms such as AliPay (online payment), Taobao (online shopping), and Meituan (online food-ordering). Unlike university students in the late 1980s, who played an important part in galvanizing social change during the democratic movements, the currently enrolled university students, mostly born after 2000, grew up in a time of rapid economic transformation and technological advancement in China. They are the generation shaped by the Chinese information society, which is characterized as a form of "authoritarian informationalism" that combines elements of capitalism, authoritarianism, and Confucianism (Jiang, 2010). As active users of social media and online services, these university students are also the subjects of mass surveillance from the state and private actors on the Chinese Internet. Their perceptions and behaviors regarding government and commercial surveillance practices are particularly relevant to an updated understanding of the Chinese surveillance society.

The research method employed in this dissertation is an analytical survey. A nationwide survey project that involves an online mode and a paper mode was conducted among currently enrolled university students in China. The purpose of the survey is to illustrate the experience of young Chinese with online surveillance and how, as inhabitants of the Chinese information society, this technologically savvy population manages personal information sharing while participating in the digital social life. In the survey, participants were asked about their concerns regarding governmental and commercial surveillance practices and their willingness to share categorized personal information with different platforms, as well as various factors that affect the relationship between surveillance concern and information-sharing behaviors. In addition, the two-mode design examines the possible existence of a mode effect in which online participants significantly differ from paper-survey participants in key factors associated with this

relationship. In this manner, the survey project helps to identify the contextualized information privacy management strategies that Chinese university students practice as they engage with social media and online service platforms, and how much of a mode effect is present in surveillance attitude survey research in the China context.

The theoretical perspectives and analytical tools of this dissertation are largely informed by the emerging field of surveillance studies, as well as recent legal and social science scholarship on theories and policies around privacy and surveillance. Believing that revisiting the concept of privacy and its purposes in the context of the surveillance society is the key to reiterating the value of privacy and formulating new regulatory approaches, this study builds its theoretical framework on research that has examined the characteristics of the modern surveillance system, the subject of privacy, and the contextual nature of privacy in the past two decades. It also seeks to interpret the Chinese surveillance society from these theoretical perspectives in the search for a more nuanced treatment of the surveillance experience in contemporary Chinese society. This chapter reviews the theoretical framework and then presents the chapter outline of this dissertation.

Understanding the Surveillance Society

The notion of the surveillance society, as argued by Lyon (2001), indicates that "surveillance activities have long since spilled over the edges of government bureaucracies to flood every conceivable social conduit" (p. 33). The surveillance society at its core is technology dependent; it is the result of communication and information technologies binding time and space in novel configurations (Lyon, 2001, p.23). Today, while government entities are still involved in many of the monitoring activities, the vast majority of data mining and processing and information trading originate in the private sector (Cohen, 2012, p.107). Moreover, there

exists a “public/private cooperation and co-optation” where the government is increasingly willing to target the owners of private infrastructure for cooperation to engage in surveillance (Balkin, 2014). It is, therefore, too restrictive to assume that the state is the predominant agent of surveillance in the digital era. Rather, the surveillance society has superseded the Orwellian totalitarian state-centered control, and is comprised of both state and non-state efforts to monitor different populations through mass surveillance (Haggerty & Ericson, 2000).

The surveillance system is fundamentally networked. It exploits correlations between behaviors and predictive cues from different corners of modern life to make connections between systems of data and integrate them into a larger system. In this sense, the surveillance system is also radically decentralized. Haggerty and Ericson (2000) refer to it as the “surveillant assemblage,” in which surveillance grows “across a series of interconnected roots which throw up shoots in different locations.” Such features of the surveillance system enable deductive, inductive, and sematic reasoning based on voluminous assemblages of data and generate new knowledge about individuals that extends beyond recorded data and the context in which such data is collected (Nissenbaum, 2019). This remarkable potential of the surveillance system is at the core of the new challenge to privacy from information and computational technologies— the system’s ability to draw new knowledge from observed phenomena using sophisticated statistical analyses.

The public’s reactions to the growing systems of surveillance, however, have not been consistent. As highlighted by Nissenbaum (2010), while some modern surveillance practices such as cameras in public places and government wiretapping are condemned and resisted by the public, other surveillance technologies that provide convenience, such as monitoring devices based on biometric data or geolocation, are celebrated. This inconsistency attests to the public’s

role in the extension of mass surveillance in modern society. A better understanding about the surveillance society requires recognition that popular support for efficient information processing has played an important role in accelerating the growth of modern surveillance. As noted by Rule (2007), the public's expectations of "justice in treatment of individuals on the bases of their full record" have greatly fueled the surveillance society (p.21). It, therefore, can be argued that the extension of mass surveillance is not simply an institutional imposition on passive publics; it is rather the result of trained public expectations for efficient interactions and transactions plus the advancement of analytical power.

The Subject of Privacy in the Surveillance Society

The initial theoretical question this dissertation seeks to address is what kind of selfhood should information policies concerning privacy and surveillance seek to promote. The dominant approaches to privacy theory traditionally consider the subject of privacy to be the autonomous individual who possesses the capacity for rational choices and self-determination. As will be explained extensively in the chapters to follow, this traditional conception of the subject of privacy is presented with fundamental challenges on both theoretical and practical levels. In this dissertation, the subject of privacy is regarded as the "networked self," which Cohen (2013) has conceptualized as the "dynamic, emergent subjectivity" that practices "socially situated boundary management." This subject is constituted by its social and political culture, which in turn shapes the form of self-determination and participation. However, the liberal self that is autonomous and the social constructed subject are not irreconcilable opposites. They are "equally implausible endpoints on a continuum along which social shaping and individual liberty combine in varying proportions" (Cohen, 2012, p. 115).

This networked self also lives in a fundamental paradox. Quantitative social science research on privacy attitudes and behaviors has identified a "privacy paradox," referring to the phenomenon that people's concerns about privacy are unrelated to their privacy behavior. Those who have substantial concerns with regard to their online privacy engage in self-disclosing behaviors that do not reflect their concerns (Norberg, Horn, & Horne, 2007; Dienlin & Trepte, 2015; Young & Quan-Haase, 2013). Although some studies did not, or only partially, support the privacy paradox due to measure construct adjustment (Baruh, Secinti, & Cemalcilar, 2017; Dienlin & Trepte, 2015; Wu, Huang, Yen, & Popova, 2012), the privacy paradox phenomenon is a perfect reflection of the conflicting situation in which the subject of privacy has to constantly balance the desire for privacy and the desire for disclosure and communication in the surveillance society. It is through this process that the subject of privacy practices socially situated boundary management.

To connect the research method with this theoretical perspective, participants' privacy concerns as users of social networking sites and online service, their information-sharing behaviors, and privacy protective behaviors are examined using established measures to test whether a privacy paradox exists. Participants' knowledge of existing norms of privacy policies are also measured and tested for a mediation effect between privacy concerns and behaviors. In addition, concerns about and acceptance of government surveillance is measured to explore whether there is a similar mechanism in the context of government surveillance. Such a study design helps to illustrate the conflicting conditions that the "networked self" experiences as it navigates through the everyday surveillance in the Chinese information society.

Contextualizing Privacy

Nissenbaum (2012)'s theory on contextual integrity has significantly informed the way privacy is conceptualized in this study. The contextual integrity framework proposes that protecting privacy means not "strictly limiting access to personal information, or assuring people's right to control information about themselves," but ensuring that personal information "flows appropriately" (Nissenbaum, 2012, p. 2). Stated simply, the context in which personal information is collected and shared matters to whether privacy is invaded or not. This is because our social life is constituted by distinct social contexts, and privacy norms, or what is considered an appropriate information sharing principle, ought to be determined by information's social contexts. The theory of contextual integrity posits that parameters such as "who sent the information, who received it, about whom it is, what types of information are involved, and the constrains imposed on them" should define contextual information norms; and it is regarded as infringing on privacy only if the contextual norms, or expectations of appropriate behaviors and practices, are violated (Nissenbaum, 2019).

An important advantage of the theory of contextual integrity is that it negates the definition of privacy as secrecy or stoppage of flow as in traditional privacy theories. Contextual integrity acknowledges at the outset the critical importance of personal information sharing in contemporary social life. It does not necessarily consider collecting and sharing, even leakage of information about persons, as privacy harm. As Nissenbaum (2019) argues, when seen as stoppage or control of flow, privacy could be so easily "traded off" against security, efficiency, public health, convenience, and so on, assuming that the advancement of those cutting-edge imperatives requires information to flow freely. However, as contextual integrity, privacy is not

in contradiction to information flows needed to promote those imperatives because it allows for flows that are appropriate in the information context in which the exchange happens.

Building on this theory, this study measures information sharing behaviors in a contextualized manner based on types of personal information and online service platforms. "Personal information" in this case is information about an identified person. The usage practice of the community defines personal information as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (European Parliament and Council, 1995, Oct 24).

In the survey, personal information is grouped into seven categories: basic demographics (age, gender, education), contact (email, phone, address, social media accounts), personal identifiers (government ID, name), personal preference (browsing/keyword search/shopping history), location (real-time location, location history), financial (bank account, debit/credit card), and health (medical history, health condition). Moreover, based on knowledge of the popular online service applications among young people in China, online service is sorted into six types: banking, shopping, ridesharing, mapping, travel ticket booking, and health management. When asking about participants' information sharing behaviors, both the information type and service type will be specified so that privacy attitudes and behaviors are captured in contextualized settings.

The Chinese Surveillance Society

The Chinese surveillance society under examination in this study does not conform to the "perniciously appealing ways of sensationalizing the Chinese Internet" (Yang, 2014). The

Orwellian rhetoric is neither an accurate description nor an informed and thoughtful way of examining the Chinese surveillance society. Neither will simplistic dichotomies of state versus society, authoritarian versus democracy, control versus freedom help to nurture insightful observations about the issues of surveillance in contemporary societies. As surveillance studies scholars have noted, the modern surveillance society, as the everyday routine surveillance that we know and experience today, is a product of modernity and the prominent features that define and constitute modernity (Giddens, 1985; Lyon, 2002). Therefore, surveillance has two faces: the fearful system that keeps track of personal lives also serves to enhance life quality and promote justice. Therefore, the "merely paranoid" and all negative perspectives on surveillance can always be challenged, and thus are "almost always inappropriate" (Lyon, 2002). Furthermore, post-structural analytical tools, such as Foucault's theory of power, have prompted theorists to ponder surveillance's role in modern society beyond mere repression and to ask whether surveillance has a productive dimension, as in whether it contributes to the shaping of modern subjects.

There is little reason why such theoretical insights cannot be applied to the post-1978 China. Contemporary Chinese society is a place where a neoliberal form of governance that aims to monitor and guide public sentiment is taking shape, and where a robust Internet industry is led by private actors, such as Alibaba, Tencent, and Baidu, who actively collect, store, analyze, and profit from the enormous amount of behavior data produced by more than 800 million Internet users. It has been noted that scholarly discussions around surveillance in China have been almost solely focused on political control by the state, while scholarship on surveillance in the Western context addresses not only the impact of surveillance on democratic development but also on issues such as neoliberalism governance, marketing, discrimination, and equality (Hou, 2017).

As a result, predominant theses on surveillance in China and the complications surrounding it remain limited, even though research on Chinese Internet has been abundant (Yang, 2014). Many examples of creeping surveillance have been given, but little theoretical novelty and imagination is provided about the lives that are under heavy surveillance from both the state and private actors.

Nevertheless, state surveillance remains an important focus of this study. China's unique political system and the lack of procedural transparency in a one-party non-democratic state, coupled with its bad record on human rights issues, invite questions about possible abuse of surveillance power and its effects on the lives of average Chinese people. To illustrate this point, the survey method employed in this study uses a special design: both a web-based and paper-based survey, identical in content, will be administered to sampled university students. This will address whether participants answer differently to the questions about surveillance and privacy in the online environment because of fear of government oversight. Moreover, questions about government surveillance concern and the perceived need for government surveillance are asked in the survey in order to determine the young generation's perception of government surveillance in relation to commercial surveillance on the Chinese Internet.

Significance of Study

The significance of this dissertation is threefold. First, theoretically, it seeks to bridge the dialogue between legal scholarship on surveillance, specifically the U.S. legal theories on freedom of speech and its relationship to privacy and surveillance, with the surveillance studies scholarship, which is largely influenced by contemporary social theories. The goal here is to establish a rich and concrete understanding of the landscape of modern surveillance and the value of privacy in such contexts. This is important because, in order to formulate meaningful

reform in information policy, theory must open itself to and address the postmodernist critique of the fundamental assumptions regarding the liberal selfhood and reconsider the relationship between selfhood and surveillance. As our understanding of surveillance and the information society in general deepen, it is critical that the value of privacy be reconceptualized beyond "the right to be left alone" as stated in Warren and Brandeis (1890) and "the right to control the flow of personal information" as advanced by Westin (2003; 2015), to address the emerging problems facing information policy on privacy and surveillance. Despite the focus on the Chinese surveillance society, much of the theoretical insights in the English-speaking scholarship are of significant reference value to this study. These theoretical considerations address problems regarding global information societies of which China is an increasingly important participant.

This dissertation seeks to turn from the one-dimensional focus on authoritarian state control to a perspective informed by surveillance studies scholarship, which views surveillance as a dynamic, decentralized system that encompasses everyday encounters in modern life across democratic and authoritarian states. State-centered censorship and control has been dominating discussions about the Chinese Internet. However, as new information and communication technologies evolve, surveillance as an expanding social control tool that has been widely employed in China is worth more attention. By examining the surveillance experience of university students, this study will demonstrate how young, educated, technologically savvy populations in China understand and react to surveillance encounters in which the state and the private industry are cooperative in enforcing mass surveillance.

Second, as an empirical investigation into the surveillance experience of modern individuals, this dissertation employs established survey instruments on concepts, such as information privacy concern, government surveillance concern, willingness to disclose personal

information, and privacy literacy, and connects the quantitative methods with legal and social theories on privacy and surveillance. Research on consumer privacy concerns and behaviors, which will be addressed in the method chapter, contributes to the manner in which concepts around privacy are measured quantitatively with good validity and reliability scores. However, they often speak more to consumer behavior models than to information policies on privacy. This study works to bridge the quantitative measures with theories on privacy's subject and context and explores the connections among concepts.

A number of published English works have addressed issues of privacy in China in various ways (Zhu, 1997; McDougall & Hansson, 2002; Yao-Huai, 2005; Cheung, 2009; Wang, 2009; Xue, 2010; Wu et al. 2011), but few have taken an empirical approach to examine the attitude and behaviors of Chinese Internet users using quantitative survey methods. The limited number of Chinese scholars who used surveys to investigate privacy behaviors (Shen 2015, 2017) focused solely on consumer behaviors. This study aims to fill this empirical gap in English literature on privacy and surveillance in China.

Lastly, with regard to policy and regulation, by examining the subject of information policy and the value of privacy in the surveillance society theoretically and empirically, this dissertation addresses the inadequacies of the current privacy policy framework and its underlying assumptions about the human self. Furthermore, it explores new ways of conceptualizing information policy that takes into consideration the socially constructed self and the highly contextualized privacy attitude and behaviors showed in contemporary inhabitants of the surveillance society. Such an endeavor entails a theoretical conversation between traditional legal theory and contemporary social theory's thinking on the social and cultural aspects of the human condition. This dissertation seeks to engage in such conversations and contribute to

discussions about the framework of information policy on privacy and surveillance in the global information society. Furthermore, because this dissertation is situated in China and among the young, educated, technologically savvy users, it will address specifically the unique characteristics of the Chinese surveillance society and the contemporary Chinese concept of privacy, which should inform law and regulations regarding surveillance and privacy in China.

Chapter Outline

This dissertation comprises five chapters. The present Chapter I is an introduction, providing the background, general framework, and aims and objectives of the study. The theoretical framework of this study is laid out in this chapter. The significance and organization of this dissertation are introduced.

Chapter 2 is devoted to a review of literature in law, social science, and surveillance studies that have informed the theories and methods used in this dissertation. Existing scholarship is synthetized into four distinctive themes: classical free speech theories and its limitation, theories and concepts of privacy, surveillance studies and the Chinese internet, and the Chinese concept of privacy. Research questions are proposed at the end of this chapter.

Chapter 3 introduces the research methods employed in this dissertation. Details of survey methods, including sampling, implementation, measures and measurement, data collection and analysis, as well as justifications for using a mix-mode survey design are explained.

Chapter 4 presents the main findings of the survey and the results of the research questions on Chinese university students' awareness and attitudes toward government and commercial surveillance, knowledge of platform privacy policies, social media and online service usage, and personal information sharing behaviors based on information categories and

platform types. This chapter also presents the differences between online and paper survey responses in key variables.

Chapter 5 reviews the findings of this study concluded from the survey project. Theoretical and methodological implications of the study results are discussed. Reflections on methods and the Institutional Review Board's review of this dissertation are also presented. Finally, limitations and suggestions for further study are discussed.

CHAPTER 2: LITERATURE REVIEW

This chapter reviews existing literature that has informed the theories and methods employed in this dissertation. This literature review covers scholarship under four distinct themes. First, a review of classical free speech theories and their relationship to surveillance lays out the traditional legal framework under which the right of privacy emerged and the harm of surveillance is identified. The limitations of this traditional approach when applied to the issues around surveillance will be addressed. The second part on conceptualizing privacy in the surveillance society reviews the primary ways in which privacy has been theorized in existing scholarship and identifies two theoretical perspectives that are particularly helpful in understanding the value of privacy in surveillance contexts: the theory of contextual integrity and the conceptualization of the subject of privacy in the surveillance society.

The third part on surveillance studies and the Chinese Internet introduces the field of surveillance studies and applies its theoretical perspectives to the study of online surveillance in China. Making such a connection is important for this dissertation because it introduces new analytical tools to the study of the Chinese internet and brings the study of internet control in China to a more sophisticated level of analysis by connecting it to the discussion of techniques of government. The last part on the Chinese concept of privacy reviews scholarship that took a cultural perspective in understanding privacy in the Chinese context. It addresses the questions that discussions on the Chinese concept of privacy have yet to answer and identifies the gap in the literature on the issue of privacy in China. Research questions are proposed at the end of chapter two.

Classical Free Speech Theories and Surveillance

The commitment to freedoms of thought, belief, and intellectual privacy lie at the foundation of classical theories on freedom of speech within the Anglo-American civil liberties tradition (Richard, 2013). The First Amendment of the U.S. Constitution as interpreted by the U.S. Supreme Court in the past hundred years strives for broader protection of free and unfettered thought and belief, prioritizing free speech over other social values with which it comes into conflict (Shiffrin, 2016, p.7). Under this tradition, the expansion of surveillance in modern societies is harmful to this tradition in two ways. First, surveillance by government and private actors threatens freedom of thought by creating a "chilling effect" that stifles the "breathing space" that free speech needs in order to survive. Second, surveillance creates a power imbalance between the watched, often understood in individual terms, and those who are watching, and increases the risk of an Orwellian tyranny (Richard, 2013). This understanding of surveillance heavily influenced the prevailing form of analysis about the emerging surveillance practices and its relationship to privacy. It is therefore necessary to revisit this literature and examine its place in contemporary understanding of surveillance in the information society.

Freedom of speech has been interpreted to promote many values including truth-seeking self-governance, autonomy, tolerance, and associated cultural values. The three prominent theories of free speech include the marketplace of ideas theory derived from the work of John Milton (1644) and John Stuart Mill (1966), self-governance theory developed by American philosopher Alexander Meiklejohn (1961), and a general theory of individual autonomy addressed by many scholars including Ronald Dworkin (1988) and Edwin Baker (2010). Under each theory, scholars have developed extensive arguments as to why society should grant individuals the greatest possible rights to freedom of thought and belief in the form of free

speech. Nevertheless, these mainstream free speech theories have been challenged by theoretical development in fields like feminist theory, critical race theory and literary theory, as well as by social science studies on human behaviors, leaving the traditional liberal political theory's picture of the "atomistic individual" in doubt (Bunker, 2001, p.100).

Marketplace of ideas

Marketplace theory is by far the most widely acknowledged and the most questioned theory on free speech. It posits that there exists a free market for ideas where different views and opinions can battle with each other and, given enough time, truth will eventually win out as a result of free competition. As stated in Justice Holmes' famous dissenting opinion in *Abram v. United States* (1919), "The ultimate good desired is better reached by free trade in ideas," and "the best test of truth is the power of the thought to get itself accepted in the competition of the market."

Marketplace theory finds its root in the enlightenment philosophy. In an article titled *What is Enlightenment?,* Immanuel Kant (1784) called for the public use of reason in bringing about enlightenment and argued that enlightenment is almost inevitable if freedom is allowed. The enlightenment philosophers believed that reason is a distinct capacity and property of the human mind and called upon humanity to use reason to think for itself and to discover the truth for itself instead of following what the authorities had to announce. Likewise, marketplace theory invests heavily on human rationality in telling truth from falsity in the battle between received views and new ideas in the marketplace, an idea that has been described as "wildly optimistic" (Bunker, 2001, p.6).

Marketplace theory is also under siege because it presupposes a transcendent, nonrelative "Truth" and fails to address power relations in the marketplace. This is especially relevant under

the topic of surveillance because, looking from a postmodernist perspective, it is primarily power that determines the production of discourses of truth. As stated by philosopher Michel Foucault (1980), "We are subjected to the production of truth through power and we cannot exercise power except through the production of truth" (p. 93). In other words, truth is what is allowed to have truth effects by the powerful in a society. The marketplace is never actually free and equal in terms of access and power. Certain dominant groups could have enormous control over the mass media and exclude viewpoints that challenge the status quo (Bunker, 2001, p.8). Most importantly, under the marketplace logic, privacy restrictions would be deemed as barriers to truth-discovery and efficiency, hampering markets from responding to consumer preferences (Cohen, 2012, p.11). Thus, the marketplace justification for free speech encourages personal-information processing, and is therefore often antithetical to privacy protection.

Self-governance

Self-governance theory regards freedom of speech as the means by which democracy functions. It premises that citizens in a democratic society should have access to information and knowledge relevant to issues of public concern in order to make informed decisions about their lives. Under self-governance theory, the protection offered by the First Amendment to speech is to encourage the "fullest participation in understanding of those problems with which the citizens of a self-governing society must deal" (Meiklejohn, 2000, p.88). As such, self-governance theory favors protection of speech for public purpose over private speech. Meiklejohn later responded to this critique by including artistic, scientific, and cultural expressions into the realm of public speech (Meiklejohn, 1961). A larger criticism against self-governance theory centers around its casting free speech into an instrumental role on its usefulness to voters (Bunker, 2002, p. 10). Moreover, as a democracy-based theory, self-governance theory contextualizes freedom of

speech in a democratic society, specifically in the American model, which renders it a justification that can hardly transcend the world of Western democracies.

Self-governance theory is not well-equipped to respond to the issues around surveillance for several reasons. First, political power infiltrates every aspect of modern life including not only state institutions, such as governments, police, and courts, but also schools, hospitals, prisons, and in the streets under surveillance cameras. Postmodernist analysis of power calls into question the traditional identification of power with political power and the concentration of power analysis on state institutions (Lemke, 2011, p.10). Second, like in marketplace theory, self-governance theory commits to "an abstract and disembodied vison of the self," one that possesses the possibility of "rational value-neutrality" (Cohen, 2012, p.4). Such an atomistic individual with certain claims of autonomy from power relations has been posited as the basis for extensive individual rights by liberal theorists from John Locke to John Rawls (Bunker, 1996). This "liberal self" is challenged by the structuralism notion of the human self that is constructed by culture or language, and by communitarian views of the human self that is created and realized through community and society in which individuals are raised. This tension between the autonomous self and the socially constructed self is at the core of the debate on information policy between legal theory and contemporary social theory. Nevertheless, the autonomous human self underlines much of the classical free speech theories, including individual autonomy theory.

Individual-autonomy

Individual autonomy, especially the non-consequentialist approach, may be the most relatable among the classical free speech theories to issues of surveillance, large because of its underlying Kantian moral imperative approach to individual freedom and dignity. Under the

nonconsequentialist approach, freedom of speech is an end in itself rather than a means to achieve a collective good (Baker, 1989, p.5). It recognizes freedom of speech as a moral imperative to regard individuals as rational and autonomous beings. In other words, freedom of speech underlines what it means to be human; it is valuable even if it does not in fact further human development. Individual autonomy theory therefore argues for freedom of thoughts as a moral imperative primarily centered with the individual, which makes it less susceptible to critiques that the liberal self is an inaccurate representation of individual compared to the other two theories (Bunker, 1996). Thus, individual autonomy theory could be a strong analytical tool to deploy when it comes to excessive mass surveillance of personal information and activities.

These three classical free speech theories, which generally reside in the tradition of liberal political theory, display some common weaknesses such as the assumption of an abstract, atomistic, disembodied human self and a one-dimensional static power relation. However, because classical free speech theories have been very wary of the expansion of government power over individual rights and freedoms, they are relevant where governments operate surveillance programs on individuals' personal information and communication (e.g. NSA mass surveillance programs targeting citizens of the U.S. and other countries) and arguably very helpful in pushing back at state surveillance. In such scenarios, classical free speech theories provide sufficient theoretical justifications for containing government surveillance power and protecting individual rights to freedom of thought and intellectual privacy.

However, in addressing the harms of modern surveillance technologies and practices, classical free speech theory is lacking in many ways. First, surveillance practices in our time have spread beyond nonconsensual state monitoring and become what Bauman and Lyon (2013) calls "liquid surveillance," in which individuals sometimes willingly allow and participate in

automated data collection and monitoring, and government and nongovernment surveillance deeply intertwined. Therefore, the solution to the problems of surveillance can no longer be confined to regulation of government actors, as classical free speech theories have focused on. Under the new-school speech regulation (Balkin, 2014), state and private surveillance are related parts of the same problem. Thus, classical free speech theories and First Amendment law, which requires state action to be invoked, is not sufficient in addressing the complex and dynamic power relations involved in modern surveillance practices.

Second, as mentioned above, classical free speech theories' heavy investment in the rational autonomous individual is inadequate in understanding the surveillance subject that is the modern individual. Philosophies after structuralism have generally understood the human self as socially constituted, an extension of the structure and community in to which one is born and raised. From the Foucauldian notion of panopticon, referring to the modern society since the late nineteenth century, individuals have been placed in a state of constant visibility and become the "object of information, never a subject of communication" (Foucault, 2012, p. 200). The autonomy of the modern individual is highly limited under this poststructuralist view of power and control in modern society. Therefore, to properly examine the individuals under surveillance, the traditional conception of the liberal self needs to be accommodated to address the challenges brought by postmodern notions of the surveillance subject.

Finally, there exists a strong cultural tendency in classical free speech theories to associate freedom of speech solely with liberal democracy, featuring the right to free speech and privacy as honorable characteristics that distinguish Western democracies from authoritarian regimes in the world. As Fish (1994) argued, in the rhetoric of American life, free speech is filled with political agendas that people with certain political ideology wish to advance; it is a "label"

that people only wish their favorite to wear (p.102). As such, discussions about the value of free speech seldom reach beyond the limited number of countries in North America and the Europe. However, as noted by Richards (2013), in today's world, authoritarian regimes are not the only institutions that wish to surveil; democratic governments in the West have committed to monitoring the public in the name of counter-terrorism and protecting cybersecurity. The Orwellian Big Brother shows itself in both forms of governance in the surveillance age. This is crucial to acknowledge if any substantial understanding is to be obtained about what modern surveillance is and what its purposes are.

Conceptualizing Privacy in the Surveillance Society

Surveillance, as "the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as means of influencing and managing people and population," makes visibility a social and a political issue in a new way (Lyon, 2002). Surveillance invites the question of privacy. Yet privacy, as a concept and a way to frame the various challenges brought by a growing surveillance society globally, has been widely criticized for being profoundly inadequate in the face of the challenges brought by surveillance. Like the classical free speech scholarship, privacy scholarship tends to be dominated by legal approaches and methods, and is therefore faced with serious critique from the surveillance scholarship. Much of the critique of privacy, interestingly, resembles those received by free speech theories: reliance on the liberal assumption about the human self or subjectivity, too implicated in right-based discourse, culturally relative, and ultimately practically ineffective (Bennett, 2011).

Addressing the critique of privacy scholarship, including individualism, spatial metaphors, and human right rhetoric, Bennett (2011) pointed out that the privacy value in fact has been "reframed at a governance level to meet the collective challenges posed by the

broadening and deepening of surveillance." Although some surveillance studies scholarship has been resistant to the concept of privacy to the extent of intentionally avoiding using the term (Aas, Gundhus, & Lomel, 2008), discussion around the regime of privacy is unlikely to go away because, for all the critique, it can still "displays a remarkable resilience as a way to regulate the processing of personal information by public and private organization" (Bennett, 2011).

The concept of privacy and its value in the surveillance context is a crucial component of this study because of its focus on the individual experience with personal information gathering and surveillance by state and private actors. The following sections will discuss how privacy has been theorized in recent scholarship and the conceptual adjustments that have been made to address the challenges brought by the emerging surveillance society. Three important theoretical perspectives will be addressed in this section: Alan Westin's privacy constructs, Helen Nissenbaum's theory of contextual integrity, and Julie Cohen's conceptualization of the subject of privacy in the surveillance society.

Westin's Privacy Constructs

As one of the first and most comprehensive inquiries into privacy and its value, Alan Westin (2015) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"; it is a "temporary withdraw" from society "in a state of solitude or small-group intimacy or reserve" (p.5). Westin's *Privacy and Freedom* was first published in 1967. Writing during the Cold War, Westin presented a quite individualist view of privacy and consequentially created a binary opposition between democratic societies, where individual privacy is mostly valued, and authoritarian societies, where almost no privacy is granted to individuals (p. 25). On the social-cultural level, privacy was regarded as an arena of democratic politics related to the social

legitimacy of government. On the individual level, privacy was connected with individual life in Western democracies, emphasizing that the individual's right to choose between self-revelation and reservation is essential to self-development. Such theorization of privacy, one that echoes strongly with the classical free speech theories of democratic governance and self-realization, is an essential component of the framework on which current privacy policies are built.

In addition to his theoretical contributions, Westin conducted a series of public opinion surveys that helped to build the basis for how privacy is measured and regulated in the U.S. In his series of survey research, Westin introduced three categories of individuals in relation to privacy—fundamentalist (high privacy concern and high distrust in privacy protections), pragmatists (mid-level concern and distrust), and unconcerned (low concern and distrust)—based on respondent answers to three questions about privacy concerns. Using this categorization, Westin testified to the U.S. Congress that privacy policy should focus on the "privacy pragmatists" who are willing to trade privacy off against other gains (Martin & Nissenbaum, 2016). Westin's characterization of privacy pragmatist as "Homo Economicus" who try to maximize the expected utility of personal information in the market through consumer choice, and who would favor a notice and choice approach to privacy policies (Hoofnagle & Urban, 2014), laid the foundation for privacy policies in the U.S. This framework had since greatly influenced the privacy policies model of today's Internet platforms across the world. Westin's substantial contribution to the study of information privacy is highly respected today, but his methodologies and the underlying assumption about the privacy in his public opinion survey research has been criticized in recent scholarship.

Martin & Nissenbaum (2016) pointed out that terms such as "pragmatists" or "unconcerned" helped to forge the incorrect understanding that individuals are willing to trade

privacy off against free services or other benefits, a mentality from which companies and regulators made individual choices the nexus of regulation. As a result, the burden on privacy regulators to commit to protecting privacy rights is lessened because the focus of privacy policy is shifted to informed choices rather than the more fundamental question of whether privacy as an important social value is in fact protected by such polices. Hoofnagle & Urban (2014) made a special note on the nature of Westin's series of survey research, highlighting that these research were largely tailored to address public policy issues concerning their various sponsors and were rarely published in academic journals. Despite the problems, Westin's recognition of privacy as a liberal value and its essential place in modern society has been described as "prescient" in its time (Solove, 2015).

Privacy as Contextual Integrity

Nissenbaum (2010) parted way from Westin's notion of privacy protection, which entails "strictly limiting access to personal information or assuring people's right to control information about themselves" by proposing that privacy ought to be considered in terms of contextual integrity (p. 2). Paying particular attention to the context in which privacy is expected, Nissenbaum proposed that protecting privacy means ensuring that personal information "flows appropriately" based on "context-relative information norms" (p. 129). From this perspective, privacy does not mean that no information flows or that information is only allowed to flow only when the information subject consents, but that information flow is allowed as long as the actor (sender, recipient), the attributes (information types), and transmission principles (commercial or noncommercial) are legitimate in the context (Nissenbaum, 2010, p.140-147; Martin & Nissenbaum 2016).

Understood as a contextual integrity, privacy is not given away or violated simply because control over personal information is ceded; privacy is violated only if personal information is disclosed inappropriately. When an individual gives up information, it doesn't necessarily mean that he or she had given up privacy as well. As such, privacy as contextual integrity can account for the fact that people often willingly release and disclose information about themselves even when they show high concern for privacy, a phenomenon named the "privacy paradox," which has been addressed in a line of empirical research (Barnes, 2006; Norberg, Horn, & Horne, 2007; Young & Quan-Haase, 2013; Dienlin & Trepte, 2015; Baruh, Secinti, & Cemalcilar, 2017).

The theory of contextual integrity acknowledges the critical importance of personal information sharing in contemporary social life. It does not necessarily regard the collecting and sharing of information about persons, even the leakage of such information, as privacy harm. This perspective makes the theory of contextual integrity stand out in the surveillance era. As Nissenbaum (2019) argued, privacy as contextual integrity is not in contradiction to information flows needed to promote security, efficiency, convenience, public health, ect, because it allows for flows that are appropriate in the information context where the exchange happens, thus lifting privacy from its long-time loser's position when balanced against the cutting-edge imperatives in the information age.

Reconceptualizing the Subject of Privacy

In the critical legal scholarship, Cohen's conceptualization of the subject and value of privacy is a significant upgrade of the theory on privacy (Cohen, 2008; 2012; 2013). Critiquing the "liberal self" who has been "the subject of privacy theory and privacy policymaking," Cohen (2013) argued that the autonomous self that is free from its social and cultural context does not

exit and never has. What should be the real subject of privacy law and policy is a self that is socially constructed and emerged from preexisting cultural and relational basis (Cohen, 2012, p. 19). In this sense, the self could not have an autonomous core because we are born and remain situated within cultural context and power relations; privacy should also not be a fixed condition because the self's relationship to social and cultural context is fundamentally dynamic (Cohen, 2013).

What Cohen has accomplished with this theorization is to bring what she calls "a postliberal theory of selfhood" into the legal and theoretical discussions about privacy. More importantly, she pointed out that the autonomous selfhood and social shaping are not mutually exclusive. Cohen (2013) argued that recognizing that the self is socially constructed and remains situated in its cultural and social contexts does not forfeit individual autonomy; instead, it puts subjectivity correctly in the space between the experience of autonomous selfhood and the reality of social shaping. When put this way, privacy can be defined as "a function in the interplay between emergent selfhood and social shaping" (Cohen, 2013).

Cohen's critique of the liberal self does not stand alone. Bunker (1996) addressed the conception of the liberal self and its problems in thinking about theories of free speech. Solove (2013) also provided insightful critique of current privacy policies, which he argues find its root in liberal individualism that presuppose an autonomous self who are able to make informed, rational decisions about personal information sharing. This view of privacy self-management, according to Solove, is tasked with doing work beyond its capabilities because of the cognitive problems lying within the individuals and structural problems beyond individual control.

Cohen also incorporates the surveillance studies perspective in her theory on privacy, unravelling the relations between U.S. privacy theories, which are deeply rooted in the tradition

of liberal political economy, and the emerging field of surveillance studies that rely on the Foucauldian poststructuralist analysis of the relationship between surveillance and the development of situated subjects and communities (Cohen, 2015). By recalibrating the privacy subject to account for a poststructuralism notion of subjectivity, Cohen reconceptualized privacy as a protection of the "dynamic, emergent subjectivity from the surveillance efforts of commercial and government to render individuals as fixed, transparent, and predictable" (Cohen, 2013).

Under this framework, the value of privacy no longer carries the spatial implication as inherent in "the right to be left alone" (Warren & Brandeis, 1890); nor does privacy simply mean individual control of personal information flow (Westin, 2013). The value of privacy becomes the interest in the breathing room where the autonomous self practices contextualized boundary management while living through the daily surveillance of the networked society. Thus, Cohen's conception of privacy is connected with the surveillance studies scholarship that emphasizes controlling nature of contemporary surveillance while still allowing a space for autonomous self-formation and self-determination.

Surveillance Studies and the Chinese Internet

Research interests in the topic of surveillance in its modern form can be traced back to scholarship since the 1950s, but surveillance as a field of study only became salient after 9/11 (Lyon, Ball, & Haggerty, 2012, p.2). Surveillance studies is multi-disciplinary and includes a wide range of scholars across the social sciences, arts, and humanities. Building on Michel Foucault's landmark study of the emergence of modern techniques of social discipline, the analytical tools employed in surveillance scholarship reside in the poststructuralism tradition where power is deemed "a complex strategic situation in a particular society" (Foucault, 1980, p.

93). In this line of thinking, the concentration of power analysis solely on state institutions is challenged; the idea that power relations are primarily repressive is also called into question (Lemke, 2011, p.10-11).

Surveillance scholars have employed Foucault's analysis of power and control to grasp the larger operations of power within atomized, decentralized surveillance encounters (Andrejevic, 2005; Marwick, 2012; Staples, 2014). Some surveillance theorists even argue that in networked societies surveillance operations are more decentralized than Foucault's work suggests. Drawing from the work of Deleuze and Guattari (1987) on the system of social control, Haggerty & Ericson (2000) proposed the concept "surveillant assemblage," referring to the prevailing model of surveillance "abstracting human bodies from their territorial setting and separating them into a series of discrete flows," which are then reassembled into distinct "data doubles" for scrutiny and targeted intervention. This assemblage operates "across both state and extra-state institutions" instead of "exemplifying Orwell's totalitarian state-centered Oceana" (Haggerty & Ericson, 2000). The assemblage perspective transforms the purpose and hierarchies of surveillance and have led to the field's more nuanced treatment of surveillance in the Western context. However, such theoretical depth has not been observed in the narratives of surveillance in non-Western countries such as China.

Surveillance and China

Recent media coverage of surveillance in China is vivid with the image of an Orwellian dystopia (Mitchell & Diamond, 2018, Feb 2; Millward, 2018, Feb 3; Carney, 2018, Sept 17). Concerns have been raised regarding mass government surveillance in an authoritarian state, where due process and transparency are lacking compared to advanced democracies in the West. It is specially concerning when it comes to the Chinese Communist Party's treatment of political

dissidents historically and now. As have been well illustrated in recent reports on the Chinese surveillance state, the emerging virtual social credit system in China can easily be used by the state powers to punish those who are deemed the enemy of the state through total disabling of their participation in the information society (Botsman, 2017).

It is, however, reasonable to suspect that the Chinese surveillance society stretches more complicated dimensions beyond the authoritarian state and its political dissidents. As Hou (2017) observed, scholarship on surveillance in the Western context is often treated differently than in China: When academia talks about surveillance practices in the Western context their focus includes not only the impact of surveillance on democratic development but also on issues such as neoliberal governance, marketing, discrimination and equality; however, discussions of surveillance in the context of China focus almost solely on political control by the authoritarian state on its people, allowing simplistic dichotomies of state versus society and control versus freedom. As important as it is to highlight the overt state surveillance in China, discussions around mass surveillance in China requires new analytical tools and theoretical novelty in order to develop nuanced and insightful understandings about contemporary surveillance in China and the global surveillance society in general.

As has been noted, metaphors like Big Brother are outdated for surveillance power in modern society; dichotomous oppositions between freedom and security are superficial and unhelpful in facilitating insightful arguments about issues of contemporary surveillance operations (Gillion & Monahan, 2012). This is true not only for surveillance in Western democracies, but also for the novel surveillance practices and experiences in contemporary China. This dissertation argues that popular narratives of a faraway Orwellian dystopia compress the space of dialogue through which various surveillance practices across different form of

governance can be investigated, and stifles theoretical imagination for studying surveillance in China. Moreover, it has become a reality that both authoritarian regimes and democratically-elected governments in our time have committed to monitoring and managing the population through the assistance from modern surveillance technologies. In this regard, moving beyond the binary oppositions between authoritarianism and democracy might help reveal substantial insights about the nature of modern surveillance and its purpose.

Studying Online Surveillance in China

Questions about how the state deters and monitors the internet in China have attracted extensive academic attention in the English-speaking academia in the past two decades. From the early works that detailed the practices of Internet control deployed by the state against dissident activities in cyberspace (Chase & Mulvenon, 2003; Wu & Goldsmith, 2006), to empirical research that examined Chinese online censorship tactics, structure, and actors (MacKinnon, 2009; Bamman, O'Connor & Smith, 2012; King, Pan & Roberts, 2013), to critical studies that reflected on early works that overemphasized the revolutionary potential of the Internet in China (Leibolo, 2011; Lee, Liu & Li, 2013; Lee & Liu 2016; Hou, 2017), scholarly interests shifted from the digital libertarian ideal that regards the Internet as a regime-changing force in the authoritarian state to broadened discussions about Internet governance. Debates have been brought beyond issues of dissidents-versus-the state and toward more complex issues concerning power and control on the Chinese Internet.

In as early as 2003, Christopher Hughes had proposed that Chinese Internet studies apply the Foucauldian Panopticon concept to explain the culture of surveillance in cyberspace (Hughes, 2003). This call has recently been answered by surveillance studies scholars, specifically those that focus on the control practices of the Chinese Internet with an emphasis on

governance and governmentality (Vuori & Paltemaa, 2015; Hou, 2017). These new perspectives have brought the study of Chinese Internet control to a more sophisticated level of analysis by connecting it to the discussion of techniques of government for the first time.

It is important to note that the Foucauldian and Deleuzian analysis of the system of control in modern society, on which much of the surveillance scholarship is built, is very much targeted at capitalism and neoliberalism. So how could it be applied to the Chinese context? In fact, contemporary China after the "Opening and Reform" program in the late 1970s has undergone a series of dramatic social transitions. These changes led to "the abandon of the effective massline politics that characterized the Maoist era in favour of a reconfigured version of 'scientific social engineering and socialist planning' combined with neo-liberal strategies of 'governing from a distance' through the development of new technologies of the self" (Jeffereys & Sigley, 2009, p.2). In other words, China's adoption of market-based economic reforms has resulted in a "hybrid socialist-neoliberal form of political rationality," which is both authoritarian in a familiar political and technocratic sense and also seeks to govern through planning and administrative rationality (Jeffereys & Sigley, 2009, p.5). Therefore, concerns of governmentality can and need to be extended to the Chinese context to highlight the changes in the nature of the Chinese Internet governance, particularly the enactment of online security practices.

In fact, there exists a body of literature on governmentalities in China that has noted the trend of neoliberal governance, pointing to the nuanced changes that have taken place in the ways Internet content is regulated (Greenhalgh & Edwin, 2005; Jefferys, 2009; Vuori & Paltemaa, 2015). Some pointed out that China as a regime with full powers to directly censor usually avoids doing so. For example, a Harvard study discovered that the regulation practices on

the Chinese Internet intend not so much on deleting all together forbidden content, but instead focused on distraction, cheerleading, and preventing meaningful collective action (King et. al, 2013). Others have found that the post-totalitarian China protects its political core by trying to prevent public discourse on its leaders and key opponents from going viral (Vuori & Paltemaa, 2015), and utilizes the market for online opinion surveillance (Hou, 2017).

As noted by Yang (2014), our understanding of the multidimensional Chinese Internet and the dynamics of contestation surrounding it remains limited despite the abundant and still thriving research on the Chinese Internet. The reason for this limitation, Yang argues, is a bias in these studies toward "sweeping and dichotomous analytical categories," including state versus netizens and authoritarianism versus democracy (Yang, 2014). Studying online surveillance in China requires a resistance to such a binary dichotomy and a more sophisticated level of analysis informed by the surveillance studies scholarship, which is what the this research aims to achieve.

The Chinese Concept of Privacy

Understanding the value of privacy in the cultural context of China is necessary to inform future information policy on privacy in a contextualized manner. Given its long history, geographical spread, large population, and ethnic diversity, it is reasonable to suspect that there exists a wider range of variation in China about the concept of privacy (McDougall & Hansson, 2002). Chinese people at various times and places have demonstrated an acute awareness and appreciation of privacy, although the ways of thinking about privacy differ greatly in different times and places and among different groups of people.

History and literature studies have demonstrated that the Chinese concept of privacy predates the modern era. Chinese debates on the political and ethical implications of the *gong [public, public space, open, communal]* and *si [personal, self, selfish, private]* spheres go back to

the Warring States period (475-221 BC). Confucian debates about *gong* and *si* can be found in writings throughout the Tang and Song period (618-1270). Based on analyses of the vocabulary for the debate between *gong* and *si* in the Tang texts, historians noted that, acting for private interests in the public domain is always considered bad, while acting for private interests in the private domain could be either good or bad depending on circumstances (McDougall, 2002). In the twelfth century philosophical texts, the term *si* retained positive as well as negative attributes. The Song intellectual Sima Guang drew a clear distinction between *gong* and *si*, and argued that government institutions must always function in the interests of the survival of the state's political integrity, but did not propose that private interests should be challenged or suppressed for that purpose (Bol, 1993).

Confucianism as the most prominent philosophical tradition in China values intimate relationships and self-discovery. The central role of the family in Confucianism gives family a far greater doctrinal importance than it has in most Western systems of thought (Whitman, 1985). While Confucian ideology emphasizes an orderly society built on a parallel hierarchy system where people are guided toward correct attitudes and behaviors, Taoists place no comparable emphasis on family and social bounds. Instead, Taoism stresses the virtues of inwardness and of things concealed. This withdrawal is regarded as a means of survival and a necessity in troubled times (Whitman, 1985). Both Confucianism and Taoism value intimate relationships, but the ultimate goal in both philosophies is to rise above particular human ties to achieve a greater union, either with a society ordered according to the patterns innate to human nature or with the Tao (Whitman, 1985). This is distinct from the Western concept of individualism that holds that a human being is fully autonomous if he or she is allowed to discover what is distinctive about himself or herself as an individual, and the idea that people

understand themselves best when separate from others. Despite the differences between Western and Chinese conception of human autonomy, Western thoughts became an important influence on the Chinese understanding of privacy as history moved on.

The impact of Western thoughts on privacy became evident in the early twentieth century. By the late imperial era, elite awareness of a Western notion of privacy and an appreciation of its benefits had been raised (McDougall, 2002). Faced with the chaotic political conditions of the late Qing period (1840-1912), that is an old and corrupted dynasty cornered by colonial powers of the West, and the need to build a strong nation state, the late Qing intellectuals were forced to reconsider the entire cultural and social basis of the traditional Chinese society. The adoption of Western-derived notions during this time, coupled with the urgency for reformation, created a new context in which privacy was imagined in the early twentieth century China (Zarrow, 2002; McDougall, 2002).

In contemporary China, the concept of privacy very much follows its equivalent in advanced democracies where privacy is regarded as a claim of the right to be free from unwanted attention and disruptions. The right to privacy is connected with individual rights to autonomy and self-determination. In Chinese terms, it is to establish a new *si* as *gong*, a powerful private public between domestic relations and state governance. In this sense, the contemporary Chinese concept of privacy follow closely the legal theories of privacy in the West, as exemplified in the U.S. and E.U. For example, dealing first with the status of the term "privacy" in the Chinese context, Zhang Xinbao (2004) defined privacy as a legal right by which citizens' residences, inner world, financial situations, social relations, sexual life, and other matters of purely personal nature are protected from any intrusion by others. Another important scholar on Chinese privacy law Wang Liming (2012) defined privacy in a similar way, with an emphasis on privacy as a

right that belongs to individuals over their personal information and private activities that have no relation with public interest. These scholarly definitions of privacy are based on the international clauses including Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which accorded privacy the status of a basic right to all human beings.

While the Chinese legal scholarship on privacy generally applies a framework that draws heavily from legal traditions in the U.S. and E.U., the Chinese social science research on privacy commonly follows the quantitative research tradition on consumer privacy in English-speaking academia (Shen, 2015; 2015; 2017). By far, little research on privacy in China, either in English or Chinese, has incorporated the theoretical insights from traditional legal theory and contemporary social theory and applied them on meditating the value of privacy in the surveillance society. This is the theoretical and empirical research gap that this dissertation seeks to fill. As our understandings of modern surveillance technology and its relationship to the idea of privacy deepens, and as the surveillance society rapidly unfolds around the world, making such theoretical connection and conducting empirical research become an imperative before meaningful insights about the value of privacy can be gained in the new historical context.

Research Questions

Guided by the above theoretical framework, this dissertation asks three major research questions. First, it asks whether information sharing behaviors among Chinese university students are consistent with their concerns for information privacy and government surveillance. This question probes at issues around the "privacy paradox," which helps to reveal the socially constructed decision-making of Chinese university students as they engage in social media and various online service platforms. The quantitative survey results concerning information privacy

concerns, government surveillance concerns, social media and online service use, willingness to disclose personal information, adoption of protective measures, privacy literacy will help inform this research question. Secondary research questions include: (1) what is the association between concerns for information privacy/government surveillance and behaviors regarding use on social media/online services? (2) what is the association between concerns for information privacy/government surveillance and willingness to disclose personal information? (3) what is the association between concerns for information privacy/government surveillance and adoption of privacy protective measures? (4) what is the association between privacy literacy and, respectively, privacy/surveillance concerns, social media/online service use, and willingness to disclose personal information?

The second research question asks whether privacy judgments about personal information are contextualized as Chinese university students navigate through various online platforms. With the way personal information and online service platforms are categorized in the study design, this research question will help illustrate how students make contextualized decisions about information sharing based on the type of personal information being shared and the nature of the platform that requires such information. Secondary research questions include: (1) how does willingness to share personal information vary based on the type of personal information being shared? (2) how does willingness to share personal information vary based on the type of platform with whom the information is shared? (3) how does privacy efficacy vary across different types of information on social media and online service platforms?

The third research question asks how experience of state and commercial surveillance have shaped the way university students share their opinions and attitudes while on the internet, and what implications can be drawn about the Chinese surveillance society and information

policy. This research question is informed primarily by the survey design of this study. The first part of the question is answered by examining the differences in key variables between those who answered online and those who filled the same questionnaire on paper. A finding of a mode effect would suggest that knowledge and experience of online surveillance have had an impact on the way young people express themselves online, though methodological questions about using online survey methods to examine privacy attitudes and behaviors would also be implied. The final questions about implication for the Chinese surveillance society and information policy in general is answered using key findings from the survey in connection with theories on privacy's subject and purpose in the surveillance society.

CHAPTER 3: METHODS

The research method used in this dissertation is analytical survey. A nationwide mixed-mode survey—web-based and paper-based questionnaires—is employed to investigate Chinese university students' surveillance experiences and privacy behaviors. This chapter presents the research design for the study and describes the details of sampling, operational definitions, measurements, implementation, and a data analysis .

As one of the most frequently used methods in communication research, a survey, or constructed question asking, is a great tool to learn about respondents' cognitive beliefs or perceptions, factual knowledge, active feelings or emotional responses, and behaviors (Baxter & Babbie, 2004, p. 167). The survey method has the advantage of providing close estimations of the distribution of characteristics in a population by surveying only some members of that population (Dillman, Smyth, & Christian, 2014, p. 2). It helps in deciphering factors that might serve as "explanations or predictors of certain viewpoints or a particular phenomenon" through using analytical methods (Luther, 2011, p. 146).

With rapidly advancing computer technologies, online surveys have become the fastest growing form of surveying occurring in the U.S. and throughout most of the world because of the speed, low costs, and access to wide geographic areas (Dillman et al., 2014, p. 301). China is no exception to this development. Scholars have conducted successful online surveys in China by combining online survey service providers, such as Sojump and Wenjuan, and the Chinese indigenous social media application WeChat (Mei & Brown, 2017). However, nontrivial concerns have been raised about the sampling and validity of the data in web-based survey

design (Wright, 2005; Moy & Murphy, 2016), some of which are salient and need to be addressed in this study.

Using Survey to Study Privacy and Surveillance in China

Surveying people about digital privacy using online questionnaires invites methodological questions, especially those that concerns sampling. Using web-based surveys to measure an individual's attitude toward online privacy and surveillance issues may produce what is known as sample nonresponse error, which happens when the characteristics of respondents differ from those who chose not to respond in a way that influences the study's results (Dillman et al., 2014, p. 5). Indeed, research have suggested that the invasiveness of online surveys makes it highly possible that individuals with higher privacy concerns are already excluded in the sampling process (Evans & Mathur, 2005; Deutskens et al., 2006). A recent meta-analytical review on research about online privacy concerns highlighted the effect of the data collection mode (online vs. offline) on study results, indicating that studies conducted offline reported a weaker positive association between privacy concerns and the adoption of privacy protection measures than studies conducted using online methods (Baruh, Secinti, & Cemalcilar, 2017).

Another important question about online surveys is that self-selection online surveys tend to oversample younger, better educated, wealthier male urban residents (Sills & Song, 2002; Chang & Krosnick, 2009). This, however, should be less of a concern in this study because the targeted population—university students in Chinese major cities—is well suited for online methods. This population is among what Sills and Song (2002) categorized as one of the select populations who "are connected and technologically savvy" and for whom "the cost, ease, speed of delivery and response, ease of data cleaning and analysis all weigh in favor of the internet as a delivery method for survey research."

Furthermore, that this survey study takes place in China poses an interesting question about validity, one that concerns the probability of self-censorship among participants who presumably are aware of government oversight on the internet. While self-report measurements are generally subject to validity issues, concerns about participants' candidness in this specific context is a valid given the widely known "Great Firewall" on the Chinese Internet and the expanding online surveillance in recent years.

To address these methodological concerns, this study employs a mixed-mode survey design combining web-based and paper-based surveys. This approach would clarify whether a mode effect exists and if so, to what extent participants' responses differ when they respond online and when they fill in a paper questionnaire on campus. Methodologists have increasingly encouraged the use of mixed-mode surveys because they help improve response rates and reduce survey errors as technology has made coordination across modes easier and response rates to single-mode surveys has declined (Dillman et al., 2014, p. 400-403).

Sampling

The population in this survey research is Chinese university students, both at the undergraduate and graduate level. Statistics released by the Chinese Ministry of Education (2018) showed that the number of undergraduates and graduates attending regular higher education institutions in China had reached 30 million in 2017. Sampling from such a large population on a national scale requires strategic methods, such as multi-stage sampling, which allows the sample to be further reduced by selecting a sample from the clusters in the population (Kemper, Stringfield, & Teddlie, 2003, p. 279). In this survey research, multi-stage purposeful sampling was used first to select the city that hosts the most higher education institutions in each geographic area—North, South, Middle, East, and West—and then select at least two institutions

with different subject focuses in the five selected cities. This multi-stage sampling strategy effectively reduces the sample size while still capturing a range of variation at early phases of sampling (Palinkas et al., 2015).

In the first stage, Beijing (North), Guangzhou (South), Wuhan (Middle), Shanghai (East), and Xi'an (West) were selected as the cities that host the greatest number of higher education institutions (Chinese Ministry of Education, 2017). The second stage involves selecting universities with a variation of subject focuses. This is necessary because one of the special features about Chinese universities is that many are established upon their strongest subject, named accordingly, and nurture a unique culture around that subject (e.g. China Agricultural University, China University of Technology, Beijing Language and Culture University, Beijing Normal University). In addition, area of study is measured in this study as a potential factor contributing to study subjects' knowledge about privacy-invasive technologies and hence their attitude and copying strategies. Therefore, it is important to ensure that universities with different discipline marks are included in the study. However, this second stage sampling strategies was used only for the paper survey conducted on university campuses; it was not possible to apply the same strategy for the online sample because a different data collection method is used, as will be explained in the following section.

Data Collection

This study used different data collection methods for the paper-based and the web-based survey. For the web-based survey, an electronic questionnaire was distributed via Sojump, a Chinese survey platform with sample recruitment service (Mei & Brown, 2017). Sojump is by far the only survey platform that offers sample service toward university students around China. The limitation of this service is that it cannot pinpoint a specific university, which means that the

second-stage sampling strategy, which seeks to sample universities with a variety of discipline focuses cannot be realized in the web-based survey. Nevertheless, all facts considered, Sojump's sample recruitment service is the most time- and cost-efficient way of conducting an online survey in China that targets university students on a national scale.

For the paper-based survey, this study follows Dillman et al.'s (2014) mixed-mode design principles, which require using the same questions and question order to minimize differences in visual design, and used the same questionnaire design as the online survey. The printed questionnaire was distributed on campus in selected universities by an research assistant who recruited participants in person in university libraries and cafeterias. The collected paper questionnaires were then transformed into electronic questionnaires for data analysis.

In this study, online survey participants were offered platform credit and paper survey respondents were offered cash incentives for their participation. Procedures of data collection and incentive distribution were approved by the Institutional Review Board of the University of North Carolina at Chapel Hill.

Survey Measures

Eight central concepts were measured in the survey research, including information privacy concerns, government surveillance concerns, perceived need for government surveillance, social media and online service use, willingness to disclose personal information online, adoption of protective strategies, privacy efficacy, and privacy literacy. Most items were measured on a 7-point Likert scale. Privacy efficacy was measured on a 5-point Likert scale. Privacy literacy was measured using true/false/I don't know questions. Social media use and online service use were measured on a frequency basis. The items used for measuring each

concept were adopted from existing literature measuring similar concepts and adapted to reflect the context of this study

Information privacy concerns. To measure internet users' concerns about information privacy, the Internet User's Information Privacy Concerns (IUIPC) scale developed by Malhotra, Kim, and Agarwal (2004) was used to capture three dimensions of concern—collection, control, and awareness. The IUIPC is an extension of the widely acknowledged Concern for Information Privacy (CFIP) scale by Smith et al. (1996). The first dimension, *collection*, adopted directly from CFIP, captures the concerns about the amount of individual-specific data provided to online companies relative to the value of benefits received (Malhotra et al., 2004). The four-item scale asks the degree to which participants agree with statements such as "It usually bothers me when online companies ask me for personal information." The newly developed dimension *control,* defined as consumer willingness to "exercise process control and influence changes in organizational policies" (Malhotra et al., 2004), consists of four items including statements such as "I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of marketing transaction." The third dimension, a*wareness,* captures consumer concern about awareness of organizational information privacy practice. This dimension contains four items. An example statement is, "Online companies seeking information online should disclose the way the data are collected, processed, and used."

Government surveillance concerns. Concern about government surveillance refers to individual concerns about government monitoring of internet activities. This variable was measured using the Government Intrusion Concerns (GIC) scale by Dinev, Hart, and Mullen (2007), which highlighted the lack of validated instruments that measure public beliefs toward government surveillance or similar latent constructs. The GIC scale consists of three items and

showed good convergent validity and composite reliability (Dinev et al. 2007). The three items ask participants to indicate on a 7-point Likert scale the degree to which they agree or disagree with these statements: "I am concerned about the power the government has to wiretap Internet activities"; "I am concerned that my Internet accounts and database information will be more open to government/business scrutiny"; and "I am concerned about the government's ability to monitor Internet activities."

Perceived need for government surveillance. Also adopted from Dinev et al. (2007), the Perceived Need for Government Surveillance (PNGS) scale was used to measure acceptance of government surveillance. It is defined as the internet user's belief that the government needs greater access to personal information and more authority to monitor Internet activities for the purposes of safety, efficiency, and reliable internet transactions. The four-item scale consists of statements including, "The government needs to have greater access to personal information/individual bank account," "The government needs broader wiretapping authority/to have more authority to use high tech surveillance tools for Internet eavesdropping." This variable was also measured on a 7-point Likert scale ranging from "Strongly disagree" to "Strongly agree."

Social media and online service use. Social media use and online service use were measured separately because previous research suggested that behaviors regarding social media and online service relate differently to concerns about privacy (Baruh et al., 2017). To measure social media use, two questions were asked regarding the frequency usage of three social media platforms—WeChat, QQ, and Weibo. Participants were asked to indicate the average time they spend per day using each of the three platforms in the past week (1= less than 10 minutes; 2= 10 to 30 minutes; 3= 31 minutes to less than 1 hour; 4= 1 hour to less than 2 hours; 5= 2 hours to

less than 3 hours; 6= 3 hours to less than 4 hours; 7= more than 4 hours). For measuring online service use, two matrix questions were used to ask participants how frequently they used six types of online services—banking, shopping, ridesharing, online travel ticketing, maps, and health management—in the past month (1= less than once a month; 2= once a month; 3= a few times a month; 4= once a week; 5= a few times a week; 6= once a day; 7= several times a day). The categorization of online services was based on general knowledge about the popular online platforms in China among young people.

Willingness to disclose personal information. Personal information refers to the individual-specific data that is the primary source of consumer privacy concerns and includes five broad categories: demographic characteristics, lifestyle characteristics, shopping habits, financial data, and personal identifiers (Phelps, Nowak, & Ferrell, 2000). The categories were adopted and modified to reflect the context of Chinese university students. Accordingly, participants were asked to indicate how willing they were to provide to social media and online service platforms the following seven types of personal information: (1) basic demographics (age, gender, education), (2) contact (email, phone, address, social media accounts), (3) personal identifiers (government ID, name), (4) personal preference (browsing/keyword search/shopping history), (5) location (real-time location, location history), (6) financial information (bank account, debit/credit card), (7) health information (medical history, health condition). Willingness to disclose personal information was measured on a 5-point scale ranging from "Never willing" to "Extremely willing" and was measured separately for social media (WeChat, QQ and Weibo) and each type of online service (banking, shopping, ridesharing, maps, and health management).

Privacy efficacy. To measure efficacy for information privacy, which is individuals' beliefs in their ability to exercise control over own actions regarding personal information (Kuo, Lin, & Hsu, 2007), participants were asked to indicate how much control they think they have over the seven types of personal information (as listed above in "willingness to disclose personal information") on social media (WeChat/QQ and Weibo) and the online service platforms (as listed above in "social media and online service use"). All items were measured on a 5-point Likert scale ranging from "No control at all" to "A great deal of control."

Protective strategies. Protective strategies are conceptualized as the power-enhancing behaviors of users to defend their personal information, which according to the model developed by Wirtz, Lwin, and Williams (2007) includes three individual actions: fabricate, protect, and withhold. The dimension *fabricate* refers to a user's effort to hide his or her own identity by providing fictitious or false information and is measured with three items including statements such as "I would consider making up fictitious responses to avoid giving websites real information about myself." *Protect* refers to the use of available software to safeguard one's web-browsing behaviors from potential intruders and is measured on a three-item scale asking if participants would "use software to eliminate cookies," "disguise identity," and prevent tracking of emails. *Withhold* captures users' refusals to provide personal information or use the online service and is measured with three items asking if participants would be "reluctant to register," "refuse to provide personal information," and "avoid using" the website or app. All items were measured on a 7-point Likert scale.

Privacy literacy. Adapted from Westin (2009) and Hoofnagle and Urban (2014), privacy literacy was measured by six items about privacy policies. Participants were asked to indicate if a statement was true, false, or if they did not know about it. These items served as a quiz that

measures participants' knowledge about what is and what is not covered in privacy policies which users must agree to upon joining a platform. Each of the true or false question frames a privacy right as being inherently available if a platform had a privacy policy. This helps to probe at the false belief that the mere presence of a privacy policy would guarantee legally enforceable privacy rights. Some example statements include "If a website or app has a privacy policy, it means that the platform cannot share information about you with other companies, unless you give the website your permission"; "If a website/app violates its privacy policy, it means that you have the right to sue the website for violating it"; "When you use the Internet to purchase products or to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements." Privacy literacy scores were between 0 and 6, with each question earning 1 marks if answered correctly.

Control variables. In addition to the common controls used in online privacy studies—age, and gender—this study also asked participants about their major in college. The list of majors is in accordance with official categories published by the Chinese Ministry of Education. Education as another common control variable is not used in this study because the study sample is heterogeneous in terms of levels of education. Instead, participants were asked to indicate which their years in university.

Data Analysis

The first step for data analysis is to establish measure reliability and validity. Reliability refers to the consistency of a measure. In this study, the internal consistency of a measure is assessed by the statistic Cronbach's α (the Greek letter alpha), which measures the consistency of participants' responses across the items on a multiple-item measure. The acceptable values for Cronbach's α are .70 and above, but a value of .80 or greater is generally taken to indicate good

internal consistency (Gliem & Gliem, 2003). Validity, on the other hand, concerns the extent to which a measure in fact assesses the variable it intended to. The validity of a measure can be judged based on various types of evidence including whether it covers the construct of interest, and whether the scores it produces are correlated with other variables they are expected to be correlated with and not correlated with variables that are conceptually distinct (Price, Jhangiani, & Chiang, 2015). In this study, factor analysis was used to test the dimensionality of scales and construct validity. Although most of the measures used in the study showed good reliability and validity in previous studies, it was necessary to run these tests since this survey was conducted in a new cultural and social context in China. In the case where an item did not load well on specific factors, the item was deleted to enhance construct validity and reliability was recalculated.

Next, because this study uses non-probability sampling. It was necessary to consider a means of compensating for the underrepresentation of certain parts of the population. Methodologists have proposed various ways for modeling and statistical adjustments, such as using weighting procedures to adjust for demographic attributes according to census demographic data of the population (Cooke et al. 2007; Chang & Krosnick, 2009; Lensvelt-Mulders et al. 2009; Pasek, 2016). However, the effectiveness of statistical adjustment is debatable. For instance, Lensvelt-Mulders et al. (2009) and Cooke et al. (2007) noted in their studies that propensity score matching and weighting would not compensate for the major difference between a random sample and a non-random sample. Some said that weighting is workable only for those who wish to evaluate relations between variables instead of looking for generalizable estimates (Pasek, 2016). It was also pointed out that the effectiveness of weighting

strategy depends on being able to identify variables that correlated with each of the variables of interest and then include them in the statistical adjustment (Baker et al., 2013).

Thus, survey methodologists have concluded that weighting is not guaranteed to improve all estimates, and that weighted data are not necessarily more representative than unweighted data (Dillman, Smyth, & Christian, 2014, p. 89). In this study, no postsurvey statistical adjustment was employed. However, during the survey sampling stage, demographic data from the Chinese Ministry of Education (2018) and campus recruitment statistics released by Wutongguo (2018) were used as references to construct a sample that matches as much the characteristics of participants to known characteristics of the population as possible. For example, the online survey sampling controlled for the number of male and female participants, as well as the number of undergraduate and graduate students so that the sample matches the overall demographics of the university student population.

To answer the research questions, basic descriptive statistics, a *t*-test, Pearson's *r* correlation, and multiple linear regression analysis were conducted using SPSS. Basic descriptive statistics for the key variables and demographics are displayed with instrument items, means, standard deviation, and level of measurement. Cronbach's alpha were reported to show measure reliability and validity. To test the association between variables, Pearson correlation coefficient was used to show the strength and direction of the linear association between privacy concerns, government surveillance concerns, perceived need for government surveillance, willingness to provide personal information, social media and online service use, protective strategies, privacy efficacy, and privacy literacy. Meanwhile, multiple linear regression analysis was used to examine whether the key variables and control variables predict willingness to

disclose personal information online. Independent sample t-test was employed to examine if significant differences existed between web-based and paper-based survey in the key variables.

CHAPTER 4: SURVEY FINDINGS

As proposed in the last section of Chapter 2, this dissertation asks three primary research questions. The first question asks about the relationship between surveillance concerns and personal information sharing behaviors and attitudes. Associations among variables including attitudes toward information privacy and government surveillance, willingness to disclose personal information, privacy protective strategies, and privacy literacy are examined to answer this question. The second research question focuses on the contextualization of privacy attitudes and behaviors among Chinese university students. This question is primarily informed by participants' responses to attitude and behavior questions in which different categories of personal information and online platforms are embedded. Finally, the third research question asks whether there are discrepancies in response between online and paper survey, which would indicate a mode effect with implications on conducting survey research on privacy and surveillance in China. The present chapter reports the findings from a national survey among Chinese university students in regard to these research questions.

Research findings are presented in five sections in this chapter. The first and second sections reports participant demographics and descriptive statistics of key variables. The rest of the chapter reports the survey findings for each of the three research questions respectively. Secondary research questions are addressed in the corresponding section. Results from statistical analyses are presented at the end of this dissertation in Appendix 1.

Sample Demographics

Before answering the research questions, it is important to first review the demographic characteristics of the study sample. In total, the sample consists of 1,204 university students from five Chinese cities that host the most higher education institutions. Among the 1,204 respondents, 728 answered a web-based questionnaire via Sojump's online survey platform, 476 filled out a paper questionnaire on campus. The geographic distribution for the paper-based survey is as follows: Guangzhou 111(23.3%), Wuhan 101 (21.2%), Beijing 99 (20.8%), Xi'an 99 (18.3%), and Shanghai 78 (16.4%). Due to IRB requirements, online respondents' IP address, which would indicate their geographic regions, were not included in the data analysis. However, according to the sample service request that was submitted to Sojump, there should be about 150 respondents each from Beijing, Shanghai, and Guangzhou, and 125 respondents each from Xi'an and Wuhan.

Table 1 displays the participant demographics. Throughout this chapter, *M* refers to the mean value of a variable and *SD* refers to the standard deviation of a variable. The survey sample has an average age of 21.6 (*SD*=2.15), with the majority (95.5%) ranging from 18 to 25. The paper-based sample has more respondents over age 25 (4.8%) than the web-based sample (2.8%). The whole sample consists of more female students (54.2%) than male students (42.4%). About 3.4 percent of the respondents chose not to report their gender. This gender ratio fits the census statistics released by Wetongguo (2018), a national research institute on Chinese university students' employment status, in which the females took 52 percent and males 48 percent.

The majority of the sample is undergraduate students (66.9%), while about one third (32.1%) is graduate students. According to the numbers of students in higher education

institutions reported by Chinese Ministry of Education (2018), undergraduate students took 86 percent and graduate students took 14 percent. The web-based sample matches the overall characteristics of the university student population in terms of the ratio between undergraduate and graduate students (undergraduate 81.3% and graduate 17.2%). The paper-based sample consists of more graduate students (55%) than undergraduate students (44.7%).

Respondents were also asked about their major in university. The top five majors are engineering (21.4%), economics and management (17.3%), media and journalism (14.5%), science (10.3%), and literature (9.1%). Among the 12 categories, philosophy (1.2%) and history (0.8%) are the two majors that have the lowest percentages. This sample characteristic matches statistics reported by the Ministry of Education (2017), which states that engineering, management, and literature were the three most popular majors while philosophy was the most marginalized in undergraduate education in China.

Descriptive Statistics

The survey questionnaire in this study measures eight central concepts around online privacy and surveillance. Information privacy concerns, government surveillance concerns, and perceived need for government surveillance are measured to indicate general attitudes toward commercial and government surveillance. The results show that, on a scale from 1 to 7, the surveyed students had higher concerns for information privacy on internet platforms (M=5.81, SD=.68) than they did for government surveillance (M=4.81, SD=1.20). Both measures showed good internal consistency assessed by Cronbach's α with values of .80 and higher.

Perceived need for government surveillance captures the perceived beneficial components of surveillance and the phenomenon that internet users may encourage and even become voluntary participants in surveillance practices (Dinev et al. 2007). For this variable,

participants scored an average of 4.79 on a 7-point scale. Although lower than its original Cronbach's α value as reported in Dinev et al. (2007), the perceived need for government surveillance measure showed satisfactory Cronbach's α value of .76. As explained in Chapter 3, Cronbach's α measures the consistency of participants' responses across the items on a multiple-item measure. A Cronbach's α value higher than .70 shows that a measure has satisfactory reliability.

For social media and online service usage, participants were asked to indicate how often they used three social media platforms in the past week and how often they used six online service platforms in the past month. The results indicated that the participants are much heavier WeChat users (*M*=5.49, *SD*=1.54) than they are QQ (*M*=3.48, *SD*=1.91) and Weibo (*M*=3.58, *SD*=1.88) users. Among the six types of online services, online banking is the most frequently used service (*M*=6.11, *SD*=1.38), followed by online shopping (*M*=5.00, *SD*=1.35), online maps (*M*=4.08, *SD*=1.27), online ride sharing (*M*=3.37, *SD*=1.49), and online health management (*M*=2.77, *SD*=1.81). Online ticket booking was the least frequently used type of online service among the surveyed students (*M*=2.73, *SD*=1.12).

Willingness to disclose personal information is measured for different types of person information. Results show that among the six types of person information, basic demographic information is the one that the surveyed university students are most willing to disclose (*M*=3.14, *SD*=.82). Willingness to disclose location (*M*=2.89, *SD*=.78) and contact (*M*=2.71, *SD*=.74) lies in the middle ground. The mean value for willingness to disclose personal preference (*M*=2.37, *SD*=.81), personal identifier (*M*=2.15, *SD*=.69), and health information (*M*=2.15, *SD*=.84) are below the midpoint on a 5-point scale. Financial information was found to be the least willing to disclose (*M*=2.03, *SD*=.68) among the surveyed university students.

For privacy efficacy, which measures individuals' belief in their ability to control own actions regarding personal information, participants indicated higher sense of control over personal information on social media (*M*=2.71, *SD*=.78) than they did with online service platforms (*M*=2.58, *SD*=.82). Regarding adoption of protective strategies, which refers to the power-enhancing behaviors of internet users to defend personal information, a 9-item scale is used to measure three dimensions of protective strategies: fabricate, protect, and withhold. The mean value for protective strategies is 3.84, with a standard deviation of .85. The protective strategies scale showed satisfactory reliability measured by a Cronbach's value of .73.

For privacy literacy, it is appropriate to say that the surveyed Chinese university students failed the privacy knowledge quiz. The results show that, on a scale from 0 to 6, respondents have an extremely low level knowledge about platform privacy policies (*M*=.74, *SD*=1.07). Only 8.2 percent of respondents answered three or more of the six questions correctly. More than half of respondents (57.1%) answered every one of the six questions incorrectly.

Surveillance Concerns and Personal Information Sharing (*RQ1*)

The first research question concerning surveillance concerns and personal information sharing attitudes and behaviors has five secondary research questions. *RQ1.1* and *RQ1.2* ask how information privacy concerns and government surveillance concerns each relate to willingness to disclose personal information. To answer *RQ1.1*, a simple regression analysis was performed using willingness to disclose the seven types of information as independent variables and information privacy concerns as the dependent variable. Another simple regression analysis for willingness to disclose the seven types of information predicting government surveillance was performed to answer *RQ1.2.* Table 4 displays the results of the regression analysis.

A linear regression analysis examines two things: (1) whether a set of independent variables sufficiently predict an dependent variable, and (2) which independent variables in particular are significant predictors of the outcome variable. In a regression analysis, when the *p* value for *F* is below .05, the regression result is significant. The R^2 in a regression ranges from 0 to 1. Value "1" indicates that the independent variables perfectly account for all the variations in the dependent variable. The β weight shows how much the dependent variable increases (in standard deviations) when the predictor variable is increased by one standard deviation — assuming other variables in the model are held constant. When the β value is negative, it means that there is a negative relationship between the predictor and the outcome variable. The *p* value for β needs to be below .05 for a variable to be considered as a significant predictor.

As shown in Table 4, a significant regression equation was found for willingness to disclose the seven types of personal information predicting both information privacy concerns ($F(7,1157) = 20.43$, $p<.001$) and government surveillance concerns ($F(7,1164) = 20.60$, $p<.001$). Information privacy concerns are negatively related to willingness to disclose personal identifier ($\beta=-.17$, $p<.001$), preference ($\beta=-.14$, $p<.001$), and health information ($\beta=-.12$ $p<.001$), while government surveillance concerns are negatively related to willingness to disclose basic demographic information ($\beta=-.11$, $p<.05$), personal preference ($\beta=-.16$, $p<.001$), and location information ($\beta=-.15$, $p<.001$).

RQ1.3, *RQ1.4*, and *RQ1.5* ask how general willingness to disclose personal information is related to these key variables: commercial and government surveillance concerns, perceived need for government surveillance, use of social media and online services, privacy efficacy, adoption of privacy protective strategies and privacy literacy. To answer these three questions, a four-stage hierarchical regression analysis was conducted to predict willingness to disclose

personal information. Gender, years in college, and major in college were entered at stage one as control variables. The surveillance concerns variables (information privacy concern and government surveillance concerns) and perceived need for government surveillance were entered at stage two, social media and online service use at stage three and privacy efficacy, protective strategies, and privacy literacy at stage four. Table 3 displays the Pearson correlation coefficients for key variables and Table 5 summarizes the result of the hierarchical regression analysis.

A hierarchical regression analysis is a way to show if the variables of interest explain a statistically significant amount of variance in the dependent variable after accounting for all other variables. As shown in Table 5, the hierarchical regression revealed that at stage one, the demographic variables including gender, years in college, and major in college contributed significantly to the regression model, F (3,1097)=14,82, p<.001 and accounted for 4% of the variance (R^2=.04) in willingness to disclose personal information. Introducing commercial and government surveillance concerns and perceived need for government surveillance changed the variance explained to 16% (R^2=.16). Adding use of social media and online service slighted increased the variance explained to 17% (R^2=.17). Finally, the addition of privacy efficacy, adoption of protective strategies, and privacy literacy to the regression model changed the variance explained to 23% (R^2=.23).

When all independent variables were included in stage four, information privacy concern (β=-.19, p<.001), government surveillance (β=-.12, p<.001), and adoption of protective strategies (β=-.18, p<.001) negatively predicted willingness to disclose personal information, while perceived need for surveillance (β=.12, p<.001), online service use (β=.12, p<.001), and privacy efficacy (β=.17, p<.001) positively predicted willingness to disclose personal information. The most important predictor of willingness to disclose was information privacy concern. Social

media use and privacy literacy were not significant predictors of willingness to disclose personal information.

Personal Information Sharing in Context (*RQ2*)

The second primary research question is concerned with the contextualization of personal information sharing behavior and attitudes. In this study, the common types of personal information being shared with social media and online service platforms are grouped into seven categories: basic demographics (age, gender, education), contact (email, phone, address, social media accounts), personal identifiers (government ID, name), personal preference (browsing/keyword search/shopping history), location (real-time location, location history), financial (bank account, debit/credit card), and health (medical history, health condition). Meanwhile, the platforms where personal information are commonly shared are grouped into eight categories including two social media platforms (WeChat and Weibo) and six types of online service platforms (banking, shopping, ridesharing, maps, travel ticket booking, and health management). With these categorizations, willingness to share personal information is measured based on both information types and the platform where such information is shared; privacy efficacy is also measured separately on social media and online service platforms. Thus, three secondary research questions are proposed regarding personal information sharing behaviors and attitudes in context.

RQ2.1 and *RQ2.2* ask how willingness to share personal information varies depending on the information being shared and the platform on which the information is shared. Table 6 displays the breakdown of willingness to share personal information across information types and platforms. The results on personal information types were reported in the descriptive statistics section in this chapter. To recall, respondents are most willing to disclose basic

demographic information (age, gender, education) (*M*=3.14, *SD*=.82) and least willing to disclose financial information (credit/debit card, bank account) (*M*=2.03, *SD*=.68). Between these two are location (*M*=2.89, *SD*=.78), contact (email, phone, address, WeChat account) (*M*=2.71, *SD*=.74), personal preference (browsing/keyword search/shopping history) (*M*=2.37, *SD*=.81), personal identifier (name, government ID) (*M*=2.15, *SD*=.69), and health information (*M*=2.15, *SD*=.84).

For platform types, respondents are most willing to disclose personal information on ticket booking platforms (*M*=2.84, *SD*=.73), followed by online banking (*M*=2.75, *SD*=.76) and online shopping (*M*=2.68, *SD*=.72). Below the midpoint on the 5-point scale are WeChat/QQ (*M*=2.46, *SD*=.61), online ridesharing (*M*=2.39, *SD*=.68), online health management (*M*=2.33, *SD*=.68), and online maps (*M*=2.32, *SD*=.63). Respondents are least willing to disclose personal information on Weibo (*M*=2.16, *SD*=.66).

To further address *RQ2.1* and *RQ2.2*, Figure 1-8 shows the contextualized information sharing attitude on each platform. As illustrated in these figures, respondents' attitudes toward personal information sharing vary significantly depending on the appropriateness of the information context. For example, while willingness to disclose personal identifiers such as name and government ID is generally low on most platforms, it is relatively high on online banking and ticket booking platforms (Figure 3, Figure 7) where names and ID are essential to the service being provided. Likewise, respondents' willingness to share financial information is very low on social media platforms such as WeChat/QQ and Weibo (Figure 1-2) but relatively high on online banking platforms (Figure 7). On online ridesharing and maps platforms, willingness to share location information is the highest among all information types (Figure 5-6). On online health management platforms, willingness to share health information is the highest except for basic

demographic information which respondents are generally most willing to share across platforms (Figure 8).

RQ3.3 asks how privacy efficacy varies across information types and platforms. As displayed in Table 7, among the seven types of personal information, respondents show highest privacy efficacy on health information (M=3.26, SD=*1.13*), followed by financial information (M=3.01, SD=1.11) and personal identifier (M=2.83, SD=1.12). Privacy efficacy is low on location information (M=2.42, SD=.1.03) and contact information (M=2.35, SD=.1.03), and the lowest on personal preference (M=2.20, SD=1.06). Between social media (WeChat/QQ and Weibo) and online service (banking, shopping, ridesharing, maps, travel ticket booking, and health management), respondents showed higher privacy efficacy on social media platforms (M=2.71, SD=.78) than they did on online service platforms (M=2.58, SD=.82). Figure 9 illustrates privacy efficacy on social media and online service platforms across information types.

Web-based vs. Paper-based Survey (*RQ3*)

The third research question focuses on the differences between web-based and paper-based survey responses. RQ3.1 asks whether there are significant differences between the two survey modes on attitude variables including information privacy concerns, government surveillance concerns, perceived need for government surveillance, and willingness to disclose personal information. RQ3.2 asks whether there are significant differences on other variables including online service use, adoption of protective strategies, privacy efficacy, and knowledge about platform privacy policies. To answer these two research questions, an independent sample *t*-test analysis was used to examined the mean differences between web-based responses and paper-based responses. Table 8 displays the results of the independent sample *t*-test.

Regarding surveillance concerns, there was a significant difference between web-based responses (M=4.45, SD=1.20) and paper-based responses (M=5.36, SD=.97) in government surveillance concerns, t(1200)=-14.44, p<.001, indicating that paper-based survey respondents reported higher concerns about government surveillance than did web-based survey respondents. There was no significant difference in information privacy concerns.

A significant difference was found on perceived need for government surveillance between web-based responses (M=4.95, SD=1.10) and paper-based responses (M=4.55, SD=1.17), t(1199)=6.01, p<.001. The web-based survey respondents showed stronger belief in the necessity of government surveillance than did the paper-based survey respondents. Willingness to disclose personal information also differed significantly between web-based responses (M=2.61, SD=2.32) and paper-based responses, t(1172)=8.52, p<.001, indicating that web-based survey respondents are more willing to disclose personal information on social media and online service platforms than are paper-based respondents.

No significant difference was found in social media use or online service use between web-based and paper-based responses. Adoption of protective strategies, on the other hand, differed significantly between those who answered the web-based survey (M=3.78, SD=.86) and those who took the paper-based survey (M=3.94, SD=.82); t(1200)=-3.18, p<.001. Paper-based respondents reported using more privacy protective strategies than did online respondents.

Another significant difference was between knowledge of platform privacy policies for web-based responses (M=.68, SD=.92) and paper-based responses (M=.84, SD=1.25), t(1202)=-2.38, p=.011. Privacy efficacy also differs significantly between online respondents (M=2.82, SD=.66) and paper survey respondents (M=.84, SD=1.25),), t(1202)=-2.38, p=<.001. These findings suggest that those who answered the online survey are less knowledgeable about

platform privacy policies but reported a higher sense of control over personal information flow than those who filled out the paper survey on campus. The implications of these survey findings are discussed in the following chapter.

CHAPTER 5. DISCUSSION

The purpose of this study, as stated at the beginning chapter, is to investigate how Chinese university students experience state and commercial surveillance and how such experience has shaped their attitudes and behaviors regarding personal information sharing online. The research questions focus on three aspects: 1) the relationship between concerns about government/commercial surveillance and attitudes toward personal information sharing; 2) the situationally contextualized information sharing attitudes and behavior based on the types of personal information and the platform on which the information is shared; and 3) the discrepancies between web-based and paper-based responses in a survey study about surveillance and privacy in China and among university students.

This chapter will discuss in detail the key findings presented in the previous chapter. It will also reflect on the research method used in this study and examine the limitations. Some perspectives on future research will be discussed at the end of this chapter.

Surveillance Concerns and Personal Information Sharing

The major findings of this study in regard to Chinese university students perception of surveillance is that they found both government and commercial surveillance to be concerning to different degrees; they would also agree that government surveillance is justifiable if it is for efficiency and public safety reasons. To recall the definition and operationalization, the instruments for commercial surveillance concerns assessed beliefs about the risks and negative consequences associated with sharing personal data with private internet platforms; the government surveillance concern variable measured concerns about government monitoring of individuals' online activities and government access to personal information. The results suggested a higher concern about commercial surveillance than government surveillance. The

correlation analysis as displayed in Table 3 showed a moderate and significant positive relationship between the two types of surveillance concerns, indicating that those who were concerned about information privacy tend to be also concerned about government surveillance. In addition, perceived need for government surveillance, which measures the extent to which people recognize the beneficial aspects of government surveillance, was negatively related to both commercial and government surveillance concerns. This suggests that those who held stronger belief in justified government surveillance were less likely to consider surveillance practices concerning, be it from the government or private planforms.

As inhabitants of the Chinese surveillance society, university students nonetheless disclose a large amount of personal information on a daily basis, willingly or unwillingly, as they engage on social media and online service platforms; and the relationship between their willingness to disclose personal information and concerns about surveillance is rather complex. The privacy paradox phenomenon shows that people's concerns about information privacy do not necessarily reflect their privacy management choices such as usage of social media and online services, sharing personal data online, and engaging in privacy protective behaviors (Baruh et al. 2017; Dienlin & Trepte, 2015 Norberg, Horn, & Horne, 2007; Young & Quan-Haase, 2013). The idea of the privacy paradox suggests that there is not a unified self when it comes to people's concerns about information privacy and their actual sharing behaviors; they live in a fundamental paradox in the surveillance society.

The findings of this study showed that, among the Chinese university students, those with higher concerns over commercial and government surveillance were less willing to disclose personal information on social media and online service platforms. The correlation matrix (Table 3) showed that willingness to disclose personal information was negatively related surveillance

concerns and positively related to perceived need for government surveillance. This is further supported by the hierarchical regression analysis (Table 5) in which both information privacy concerns and government surveillance concerns were significant predictors for willingness to disclose personal information. The correlation analysis also suggested that those with higher information privacy concerns and government surveillance concerns were more likely to adopt privacy protective strategies. These findings did not reflect the conflicting self that is suggested by the privacy paradox.

However, the privacy paradox showed where surveillance concerns did not affect the amount of time that Chinese university students spent using social media use and online service use. As shown in Table 3, there was no significant correlation between usage and concerns for commercial and government surveillance. Those with higher concerns did not use social media nor online service platforms less than those with lower concerns. Furthermore, when commercial surveillance and government surveillance are differentiated and crossed over with personal information types, the relationship between surveillance concerns and willingness to disclose personal information became more nuanced.

As displayed in Table 4 and explained in findings to *RQ1.1* and *RQ1.2*, willingness to disclose demographic information was significantly negatively associated with government surveillance concerns but not associated with commercial surveillance concerns. The same pattern was observed for location information. With personal identifier and health information, however, a significant negative association showed between surveillance concerns and willingness to disclose for commercial surveillance but not for government surveillance. For personal preference, there was a significant negative association between willingness to disclose and surveillance concerns for both commercial and government surveillance. No significant

associations were found for contact and financial information. These differences suggest that participants' willingness to disclose certain types of personal information varies depending on who they are more concerned about collecting and using that information. For example, between commercial surveillance and government surveillance, participants were less willing to disclose personal identifier and health information when thinking about surveillance from private platforms, and less willing to disclose demographic information and location when concerned about government surveillance.

To sum up, this study found that the willingness of Chinese university students to disclose personal information online was significantly influenced by their concerns about commercial and government surveillance, which also drive their use of more privacy protective strategies. But, as the privacy paradox suggests, their concerns about surveillance did not affect how much they use social media and online services. These findings speak to the phenomenon that, as social media and online services become essential platforms for living and socialization in the networked society, it is increasingly difficult for the young generation to withdraw from these platforms no matter how much they are concerned about information privacy and government surveillance. In fact, against this backdrop, inhabitants of the information society enjoy very little autonomy and self-determination in regard to personal information sharing. The limited means of self-empowerment would include use of privacy protective strategies such as fabricating and disguising individual-specific information while engaging on the online platforms. But being able to exercise these measures requires that individuals have a certain level of technological knowledge and skills.

Lastly, privacy literacy in this study did not relate to willingness to disclose personal information, despite of previous research suggesting that knowledge about privacy rights might

reduce the fear to disclose personal information and hence result in higher information sharing (Park, 2013; Debatin et al. 2009; Turow & Hennessay, 2007). This is perhaps because the privacy literacy variable had a very low mean value of .07 on a 0 to 6 scale, which is evidence that Chinese university students know very little about privacy policies on their social media and online service platforms. But it is also possible that the way privacy literacy was measured in this study—using false but affirmative statements about privacy rights covered in platform privacy policies—contributed to the overall low and skewed result on this particular variable.

Contextualized Information Sharing Attitudes

The findings of this study in regard to Chinese university students' information sharing attitudes is highly consistent with what the theory of contextual integrity would suggest. The theory of contextual integrity posits that privacy is infringed not when consent is not granted as traditionally understood but when the contextual information norms or expectations of appropriate information practices are violated (Nissenbaum, 2012, 2019). The contextual information norm is determined by the sender and recipient of information, the type of information involved, and whether the information is used for commercial or noncommercial purposes (Martin & Nissenbaum 2016). In order to examine information sharing attitudes in a situationally contextualized manner, this study measured willingness to disclose personal information in a matrix of two factors: the type of information involved and the platform on which the information is shared. The results showed that Chinese university students' attitudes toward personal information sharing vary significantly depending on the appropriateness of the information context.

Before moving on to discussing the specific findings, some explanations about the contextualization is necessary. According to Phelps, Nowak, & Ferrell (2000), personal

information can be categorized as the following: demographic characteristics, lifestyle characteristics (including media habits) , shopping habits, financial data, and personal identifiers (names, address, social security numbers). In this study, these five broad categories were adapted in the Chinese context: lifestyle characteristics and shopping habits were merged into the category "personal preference," which include shopping, browsing, and keyword search habits; address was taken out of personal identifiers and merged into "contact" together with phone number and social media account; government ID was added to the personal identifier categories because social media platforms in China would ask users to register their government ID one way or another; and a new category "health information" was added to address the increasing popularity of health management applications in China, which collect and analyze individuals' basic biological indicator such as height/weight, their physical activity history, and in some cases detailed health conditions. These seven categories of personal information would cover most of the personal data that is shared online in a typical young Chinese person's daily life.

The online platforms are sorted into eight categories including the two most popular social media platforms (WeChat/QQ and Weibo) and six types of online services commonly used among young people in China. WeChat and QQ were merged into one platform because they are both owned by the Chinese tech giant Tencent and users account information is could be shared across platforms. Among the six types of online services, online ticket booking perhaps is the most unique for the China context. This is because, unlike in the United States, the absolute majority of the population relies on trains for short and long distance traveling in China. Before a national online ticket booking system was fully implemented in 2013, obtaining a train ticket on a desired date and time was highly challenging because of the almost always heavy traffic flow in China. For university students, online ticket booking platforms are essential when they travel

home during summer and winter break, which are typically the busiest times of the year for the railways. The rest of the service platforms including online banking, online shopping, online ridesharing, online maps, and online health management are utilized mostly similarly in China as they are in the United States.

By situating personal information types and online platform categories in the context of typical Chinese young people's daily lives, this study can illustrate the contextualized personal information management choices that Chinese university students make as they actively engage on social media and online services. This is an important contribution to scholarship on privacy research in China. As shown in Figure 1-8, Chinese university students' willingness to disclose personal information and their privacy efficacy are fact highly contextual based on the information types and online platforms. Aside from basic demographics such as age, gender, education, which respondents generally are willing to disclose across platforms, attitudes toward disclosing other types of personal information varied depending on the platform.

For example, on WeChat and QQ, which are social networking applications serving mainly social purposes, participants were more willing to disclose contact information than other types of personal information. On Weibo, a Chinese Twitter-Instagram mix where people follow updates from professionals and celebrities, participants were relatively more willing to disclose their personal preferences such as browsing and searching history. For online service platforms, willingness to disclose a certain type of personal information echoes the nature of the service platform on which the information is shared. For instance, participants would not mind sharing their location with interactive maps and ridesharing platforms or disclosing their health information with online health management platforms. This is contextual integrity in its concrete form in the digital life of Chinese university students.

While situated in the China context, these findings are consistent with Martin & Nissenbaum (2016) in which privacy expectations are found to be highly dependent on the contextual elements including information types, recipient, and purpose of use. What these findings have highlighted is that sensitivity of information and people's expectations for information privacy are not fixed; they are context sensitive and show many nuances in the face of confounding variables. Thus, information context, as stated by the theory of contextual integrity, ought to be a key element for determining what information privacy means and when privacy is infringed upon in surveillance age.

Studying Privacy and Surveillance in China: Survey Modes

This study found a significant difference between the web-based and paper-based survey in most key variables. Those who answered the survey online reported lower concerns about government surveillance, adoption of protective strategies, and privacy literacy than those who answered on paper; they also showed higher perceived need for government surveillance, willingness to disclose personal information, and privacy efficacy in comparison to paper survey respondents. These findings provide a valuable reference for those who wish to conduct survey research in China, especially research that focus on privacy and surveillance issues on the Chinese internet.

The mixed-mode survey design was necessary for both practical reasons and methodological concerns. From the practical perspective, the fact that this study took place in China's mainland brings out the issue of state control of the internet, of which people are generally aware. This separates China from developed Western countries in terms of people's awareness of government surveillance and the impact it might have on their risk perception when answering an online survey about surveillance. It is therefore necessary to examine whether

online respondents as a whole would answer questions differently from the paper survey respondents due to a general awareness of government oversight on the internet.

Methodologically speaking, past studies on survey methods already highlighted the possibility that people with higher privacy concerns are excluded through self-selection during the sampling stage, causing a sample nonresponse error that influences the study's results (Evans & Mathur, 2005; Deutskens et al., 2006; Dillman et al., 2014, p.5). Some reported significant differences in the strength of associations among privacy-related variables between online survey and paper survey (Baruh, Secinti, & Cenmalcilar, 2017). For these reasons, this study incorporated two survey modes and compared the differences between responses collected through online survey and paper survey.

The results of the comparative analysis, as shown in Table 8, showed that the differences between the two survey modes were mostly significant. Paper survey respondents reported higher concerns over government surveillance and lower acceptance of government surveillance. Paper survey respondents were also less willing to disclose personal information and more likely to adopt privacy protective strategies than online respondents. Despite an overall low privacy literacy across the two survey modes, paper survey respondents reported better knowledge about platform privacy policies than did online respondents. Concerns over information privacy, interestingly, did not differ between online and paper survey responses.

The differences between answers collected by online survey and paper survey indicated that awareness of government oversight on the internet may led to online respondents reporting lower concerns over government surveillance and less use of privacy protective measures; it may also contributed to higher reported support for government surveillance and willingness to disclose personal information among online respondents. One explanation could be that online

respondents had grown the habit of self-censoring and refraining from reporting concerns about government surveillance and usage of privacy protective measures. This is also evidence that experience of government surveillance had shaped the way Chinese university students share opinions and disclose attitudes in online environments.

Finally, it is necessary to note that participants of online survey and paper survey showed different demographic characteristics, which may have contributed to the differences discussed above. As displayed in Table 1, the web-based survey had more participants under age 21, more male, less graduate students, and more students who studied science, engineering, economics and management. However, given that no significant difference was found between the two modes on information privacy concerns, it is reasonable to suspect that the different responses on concerns about and perceived need for government surveillance were the result of self-censorship among the online participants.

Implications of Study

This study provides important implications on Chinese young people's experience with online surveillance, doing research on privacy and surveillance in China, and more broadly on information policy in the surveillance age.

As a survey project conducted in China's mainland and among university students, the findings of this study are largely consistent with similar research conducted in the United States and elsewhere (Dienlin & Trepte, 2015; Norberg et. al, 2007; Martin & Nissenbaum, 2016). In the past four decades of opening and social reform, China has been a keen adopter of advanced communication technologies from the West. It is surprising that decades later Chinese people's experience with the strange world of personal information gathering and digital mass surveillance resembles more than it differs from what a typical inhabitant of the information

society in the West would experience. The young generation internet users in China are confronted with the same paradox in which the desire to communicate and participate in the digital world came across with a dire realization of the conditions of mass surveillance in everyday life. Namely, their willingness to fully engage on digital media platforms, which would require disclosure of a large amount of personal information, is impeded by emerging concerns about mass surveillance from the increasingly powerful platforms as well as the traditional state institution. As a result, they apply a situationally contextualized mindset to personal information sharing practice as it became rather unrealistic for young people to fully withdrawal from the digital world. Such is a screenshot of human condition in the contemporary world that speaks across cultures and state boundaries.

The special condition of the Chinese surveillance society revealed itself in the comparison between the two survey modes in this study. Government surveillance in the Chinese context is essentially different from Western democracies because of its one-party and post-authoritarian political system. Due to a general awareness of government oversight on the internet, the Chinese young people in this study provided significantly different responses on questions about government surveillance and use of privacy protective measures when they answered online versus when they filled out the paper questionnaire on campus. This shows that awareness of government surveillance may have conditioned Chinese young people into practicing self-censorship in online environments, which is the signature of the Chinese surveillance society.

On the method level, the differences found between online and paper survey respondents in this study should remind researchers of the special nature of privacy research in the digital age. As researchers around the world are increasing inclined to use online questionnaire for its

speed, low cost, and efficiency, privacy researchers should be more cautious about using online methods because a mode effect between online and offline survey would have more significant influence on research with a focus on attitude toward privacy and surveillance than it would with other types of research. The sample nonresponse error resulted from the invasiveness of online survey is problematic for privacy research because the demographic characteristics of an online sample could be different from an offline sample in a way that would largely influence the study results; even if the demographic difference is minimized by weighting, it is possible that online respondents would report a systematically lower level of concern or other different attitudinal measures than would offline respondents because of conditions in the particular online environment in the research context. For these reasons, it may be a good option for privacy and surveillance research to employ more mixed-mode survey methods.

This study also provides insight into future information policy regarding privacy and surveillance because it sought to address some important theoretical inquiries such as what is privacy for and when is it invaded in the age of mass surveillance. Admittedly, this study eventually took the social science approach of surveying people about behaviors and attitudes toward defined concepts, and connecting social science research on privacy and surveillance to the legal scholarship has never been an easy task for research in this intersection. As Cohen (2015) pointed out, the dialogue between law and surveillance studies has been complicated by the fact that law often considers surveillance simply as the potential subject of regulation, while surveillance studies is concerned with the relationship between surveillance and social shaping and glosses over the processes of definition and compromise that regulators must confront. But one thing that might hold across the lines between law and surveillance studies is that legal

framework and doctrine shape the process of compromise that not only the law but also those who are under surveillance would have to navigate.

The opening chapter of this dissertation argued that the concept of privacy as well as its value ought to be revisited in the context of the surveillance society if the privacy challenges raised by cutting-edge surveillance technologies were to be properly addressed. Through the theoretical perspectives by scholars such as Cohen and Nissenbaum who incorporated surveillance theories into the consideration of future information policies, this study argues that the current dominant conceptions of privacy are insufficient in the age of surveillance because they misconstrued the value and purpose of privacy in contemporary life. The research findings of this study would support this argument in the following two ways.

First, the inhabitants of the information society have very limited autonomy and self-determination when it comes to disclosure of personal information on today's internet. Despite high concerns about privacy and government intrusion, individuals still would choose to engage on social media and online service platforms and disclose a wide range of personal information while doing so. This is because the networked self, as Cohen (2012) has theorized, are fundamentally confined by their social and cultural context. In a surveillance society, the subject of privacy is not the disembodied, rational, neutral, and self-determining selfhood that traditional liberal political theory would embrace. This makes the notice and choice principle in the current privacy policy framework, which makes individual choice the nexus of regulation, highly problematic. It should remind policymakers to not put the enabling and implementation of user choice in the center of the regulatory framework and invest more on examining the substantive virtues of the data practices in terms of privacy protection.

Second, in a time when online platforms have become indispensable for contemporary social life, privacy no longer means strictly restricting the flow of personal information. As shown in this study, individuals make situationally contextualized decisions based on the information type and the nature of the platform when they have to disclose personal information in order to participate in the digital world. There is not a fixed scale on which the importance of personal information can be ranked. Information that is deemed highly sensitive on one platform could be considered totally appropriate to share on another. For example, government ID is generally considered to be the type of information that should not be shared in online environments, but one would have to provide it to online booking sites when purchasing travel tickets. While it may be appropriate to share medical information with health management platforms, it is definitely reckless to disclose such information in other contexts such as one's social media. Searching and browsing histories facilitate convenient online shopping but may reveal highly private information about one's lifestyle to unwanted audience when used in other contexts.

The real challenge to privacy, however, is the information system's growing ability to synthesize information gathered from different corners on the internet to generate new knowledge about individuals that go far beyond recorded data and the context in which such data is collected. This should remind privacy policy makers that, instead of focusing on individual control over personal information on one platform, future information policy should care deeply about information sharing between platforms, which is largely out of individuals' control but nevertheless could harm privacy in fundamental ways.

Limitations

This study has several potential limitations. First, regarding sampling, this study oversampled students from highly ranked universities, female students, graduate students, and students who study media and journalism. Most of the oversampling came from the paper-based survey because the survey distribution was done by local informants who are mostly media and journalism professors and graduate students. The web-based survey participation was self-selected, which means that individuals who are not interested in the survey topic were systematically excluded from the online survey. For a study of a large population, the nonprobability sampling strategies used in this study undermines the generalizability of the findings. This study also did not ask about participants' ethnicity, assuming that the large majority would be Han, which takes about 91 percent of the population in China. It would be reasonable to suspect that people of minority ethnicities, especially those that are politically marginalized in China, would provide very different answers to questions about government surveillance. But this should be the concern of a separate research project.

Secondly, the survey questionnaire for this study, when translated into Chinese, is ten pages long. Questions about willingness to disclose personal information and privacy efficacy are contextualized based on seven types of information and eight types of platforms, resulting in ten matrix questions, which may have caused respondent fatigue. Tired and bored respondents often answer "don't know" or engage in straight-line responding (Lavrakas, 2008). Therefore the responses to the willingness to disclose personal information instruments, which are all matrix questions, and the privacy literacy instruments, which are "True/False/I Don't Know" questions, may have been compromised because of the survey questionnaire design.

Thirdly, the survey instruments used in this study were translated from its original English version into Chinese. The Chinese equivalent of the word "surveillance" is worth noting in this regard. The word "surveillance" in English carries a cultural connotative meaning of government suppression. To better capture this connotation, the Chinese translation of the survey questionnaires used the word "Jian Shi," which is often used in the context of government surveillance, instead of its synonym "Jian Kong," which means monitoring and is typically used in technological contexts such as closed circuit television monitoring. As with other important terms in the questionnaire, this study sought to provide participants with the most precise translation, but it is possible that some of the original meanings were lost in translation.

Lastly, this study is limited in its reach into the issue of government surveillance in China. The ways in which the survey questionnaire was scrutinized by the Institutional Review Board and the survey service provider have put great limits on the questions that could be asked about government surveillance. For the online survey, the questionnaire was reviewed by the survey sample service provider Sojump.com who according to law must eliminate from their online survey platform any illegal content ranging from violence, obscenity, criminal activity to inciting anti-government sentiment. For the paper survey, the Institutional Review Board required that the researcher must obtain an official approval in each university where the paper survey is distributed. Therefore, the survey questionnaire must be reviewed and approved by school officials in the Chinese universities, which means that questions about government surveillance must be carefully worded to make sure that the it is allowed to be distributed to the students.

Future Research

The continuing expansion of commercial and government surveillance in China invites extensive research on the emerging surveillance practices and the way in which Chinese people understand and experience such surveillance. However, there are practical challenges in conducting these studies. An inquiry into government surveillance issues in China that involves human subjects would exposes itself to strict IRB scrutiny in Western research institutions. A number of protective measures need to be taken to ensure that the study will not put participants' safety or employment in jeopardy, if the study were to touch on issues that are considered politically sensitive in China. Even with these challenges, there are plenty opportunities for research on surveillance in China.

For example, future research could explore attitudes and perceptions of commercial and government surveillance among different groups. The university students group, as examined in this study, has its limitation in terms of education experience and political perspectives. Future research could investigate experience of surveillance among journalists and foreign residents in China who might have different perspectives. Future research could also examine attitudes and perceptions of surveillance among the general public. Interesting differences might show between generations and between people with different level of education and privacy literacy.

Regarding research methods, future research could consider measuring actual information sharing behaviors. This study only measured intentions to share personal information, which according to literature might relate differently to privacy concerns than actual information sharing behaviors (Baruh et al. 2017). The way social media use and online service use are measured in this study could also be further developed to capture multiple dimensions of use, including satisfaction and intention for continued use.

The original research design of this dissertation included a focus group component. However, due to a strict scrutiny by the Institutional Review Board that lasted for an extensive period of time, the focus group had to be dropped from the final project. Moving forward, more qualitative research is needed to address the larger questions regarding theory and policy, as well as the cultural aspect of privacy and surveillance in the China context.

Looking beyond the China context, studies on experience with commercial and government surveillance could have a comparative perspective. For example, a comparison between the United States and China on citizen's attitudes and perceptions about commercial and government surveillance has the potential to reveal the differences, as well as the fundamental similarities between the two countries in terms of mass surveillance on its people.

APPENDIX 1. TABLES AND FIGURES

Table 1 Sample Demographics

Variable	Web-based (*N*=728)		Paper-based (*N*=476)		All respondents (*N*=1204)	
	N	*%*	*N*	*%*	*N*	*%*
Age (*M*=21.6 *SD*=2.15)						
18-21	444	61.0	166	34.9	610	50.7
22-25	263	36.1	274	57.6	537	44.6
26-29	20	2.7	22	4.6	42	3.5
30+	1	0.1	1	0.2	2	0.2
Gender identity						
Male	350	48.1	160	33.6	510	42.4
Female	363	49.9	290	60.9	653	54.2
Other	15	2.1	26	5.4	41	3.4
Geographic region						
Guangzhou (South)	-	-	111	23.3	-	-
Wuhan (Middle)	-	-	101	21.2	-	-
Beijing (North)	-	-	99	20.8	-	-
Xi'an (West)	-	-	87	18.3	-	-
Shanghai (East)	-	-	78	16.4	-	-
Undergraduate/graduate						
Undergraduate students	592	81.3	213	44.7	805	66.9
Graduate students	125	17.2	262	55.0	387	32.1
Unclassified	11	1.5	-	-	11	0.9
Major in university						
Engineering	209	28.7	49	10.3	258	21.4
Economics & Management	163	22.4	45	9.5	208	17.3
Media & Journalism	21	2.9	153	32.1	174	14.5
Science	91	12.5	33	6.9	124	10.3
Literature	49	6.7	61	12.8	110	9.1
Other	50	6.9	47	9.9	97	8.1
Law	31	4.3	42	8.8	73	6.1
Art	17	2.3	26	5.5	43	3.6
Education	32	4.4	6	1.3	38	3.2
Medicine	34	4.7	3	0.6	37	3.1
Philosophy	9	1.2	6	1.3	15	1.2
History	6	0.8	4	0.8	10	0.8

Table 2. Descriptive Statistics for Key Variables

Variable	*N*	Range	Mean	*SD*
Surveillance concerns				
Information privacy concerns (α=.80)	1194	1-7	5.81	.68
Government surveillance concerns (α=.82)	1201	1-7	4.81	1.20
Perceived need for government surveillance (α=.76)	1201	1-7	4.79	1.14
Social media use	1198	1-7	4.18	1.14
WeChat	1202	1-7	5.49	1.54
QQ	1201	1-7	3.48	1.91
Weibo	1201	1-7	3.58	1.88
Online service use	1202	1-7	4.01	.86
Online banking	1204	1-7	6.11	1.38
Online shopping	1204	1-7	5.00	1.35
Online ridesharing	1204	1-7	3.37	1.49
Online mapping	1202	1-7	4.08	1.27
Online ticket booking	1203	1-7	2.73	1.12
Online health management	1203	1-7	2.77	1.81
Willingness to disclose personal information	1174	1-5	2.50	.56
Basic demographic	1197	1-5	3.14	.82
Contact	1198	1-5	2.71	.74
Identifier	1198	1-5	2.15	.69
Preferences	1191	1-5	2.37	.81
Location	1196	1-5	2.89	.78
Financial	1198	1-5	2.03	.68
Health	1194	1-5	2.15	.84
Privacy efficacy	1192	1-5	2.64	.74
Social media	1198	1-5	2.71	.78
Online services	1196	1-5	2.58	.82
Protective strategies (α=.73)	1202	1-7	3.84	.85
Fabricate	1204	1-7	4.30	1.14
Protect	1204	1-7	3.39	1.16
Withdraw	1204	1-7	3.84	1.21
Privacy literacy	1204	0-6	.74	1.07

Table 3. Pearson Correlation Coefficient for Key Variables

	1	2	3	4	5	6	7	8	9
1. Information privacy concerns	1								
2. Government surveillance concerns	.25**	1							
3. Perceived need for government surveillance	.03	-.19**	1						
4. Willingness to disclose personal information	-.27**	-.28**	.16**	1					
5. Social media use	-.03	.01	.06	.88	1				
6. Online service use	-.04	.03	.02	.12**	.16**	1			
7. Privacy protective strategies	.16**	.22**	.02	-.23**	.01	.03	1		
8. Privacy efficacy	-.11**	-.16**	.12**	.25**	.04	.00	.06*	1	
9. Privacy literacy	-.08**	-.09**	-.01	-.01	-.03	.04	-.04	-.09**	1

** Correlation is significant at the 0.01 level
* Correlation is significant at the 0.05 level

Table 4. Summary of Simple Regression Analyses for Willingness to Disclose Personal Information (WTD) Predicting Information Privacy Concerns and Government Surveillance Concerns

	Information privacy concerns			Government surveillance concerns		
Variable	*B*	*SE*	*β*	*B*	*SE*	*β*
WTD demographic info	.05	.03	.06	-6.29	.05	-.11*
WTD contact info	-.01	.04	-.01	-5.33	.07	-.02
WTD personal identifier	-.16	.04	-.17**	-.67	.07	.01
WTD preference	-.11	.03	-.14**	4.56	.05	-.16**
WTD location	.05	.03	.06	6.38	.06	-.15**
WTD financial info	-.07	.04	-.07	-6.40	.07	.06
WTD health info	-.09	.03	-.12*	-1.04	.05	-.04
R_2		.11			.11	
F		20.43**			20.60**	

*p<.001, **p<.05

Table 5. Summary of Hierarchical Regression Analysis for Variables Predicting Willingness to Disclose Personal Information

	Model 1			Model 2			Model 3			Model 4		
Variable	*B*	*SE*	*β*	*B*	*SE*	*β*	*B*	*SE*	*β*	*B*	*SE*	*β*
Gender[a]	.13	.03	.117**	.10	.03	.09**	.09	.03	.08*	.10	.03	.09*
Years in college	-.05	.01	-.16**	-.04	.01	-.14**	-.04	.008	-.14**	-.03	.01	-.11**
Major in college[b]	-.034	.034	-.03	-.04	.03	-.03	-.03	.03	-.03	-.05	.03	-.04
Information privacy concerns				-.19	.02	-.23**	-.18	.02	-.23**	-.154	.02	-.19**
Government surveillance concerns				-.08	.01	-.17**	-.08	.01	-.17**	-.06	.01	-.12**
Perceived need for government surveillance				.06	.01	.13**	.06	.01	.13**	-.6	.01	.12**
Social media use							-.10	.01	-.20	-.10	.01	.02
Online service use							.07	.02	.12**	.08	.02	.12**
Privacy efficacy										.13	.02	.17**
Adoption of protective strategies										-.12	.02	-.18**
Privacy literacy										-.02	.01	-.18
R_2		.04			.16			.17			.23	
F for change in R_2		14.82**			52.80**			8.48**			25.47**	

[a] Male=1, Female=0

[b] Science, engineer, media & journalism=1, Philosophy, law, education, literature, history, art, agronomy, medicine, management, other=0

*p<.001, **p<.05

Table 6. Willingness to Share Personal Information Across Information Types and Platforms

	Basic demographics		Contact		Personal identifier		Preference		Location		Financial		Health		Average	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
WeChat/QQ	3.57	.87	2.81	.97	1.89	.94	2.52	1.06	2.49	1.02	1.71	.90	2.21	1.06	2.46	.61
Weibo	3.11	1.2	2.26	1.05	1.60	.81	2.36	1.11	2.28	1.07	1.50	.76	2.00	1.00	2.16	.66
Banking	3.39	1.01	2.98	1.09	2.80	1.22	2.48	1.09	2.56	1.08	2.81	1.22	2.20	1.04	2.75	.76
Shopping	3.14	1.07	3.07	1.10	2.20	1.04	2.99	1.21	2.85	1.14	2.48	1.14	2.01	1.02	2.68	.72
Ridesharing	2.73	1.15	2.66	1.13	1.96	1.01	2.01	1.00	3.44	1.18	1.96	.98	1.95	1.04	2.39	.68
Maps	2.65	1.16	2.42	1.12	1.73	.87	2.12	1.06	3.37	1.14	1.71	.84	1.89	.97	2.32	.63
Ticket	3.33	1.10	3.29	1.11	3.31	1.17	2.22	1.05	3.21	1.16	2.43	1.14	2.05	1.07	2.84	.73
Health	3.21	1.14	2.19	1.01	1.70	.85	2.22	1.11	2.55	1.19	1.60	.76	2.83	1.35	2.33	.68
Average	3.14	.82	2.71	.74	2.15	.69	2.37	.81	2.89	.78	2.03	.68	2.15	.84	2.50	.56

Table 7. Privacy Efficacy Across Information Types and Platforms

	Basic demographics		Contact		Personal identifier		Preference		Location		Financial		Health		Average	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Social media	2.37	1.21	2.38	1.18	2.97	1.28	2.17	1.18	2.51	1.18	3.17	1.26	3.36	1.26	2.71	.78
Online services	2.45	1.19	2.32	1.13	2.69	1.26	2.22	1.21	2.33	1.17	2.84	1.27	3.16	1.28	2.58	.82
Average	2.41	1.07	2.35	1.03	2.83	1.12	2.20	1.06	2.42	1.03	3.01	1.11	3.26	1.13	2.64	.74

Figure 1. Willingness to Share Personal Information on WeChat/QQ

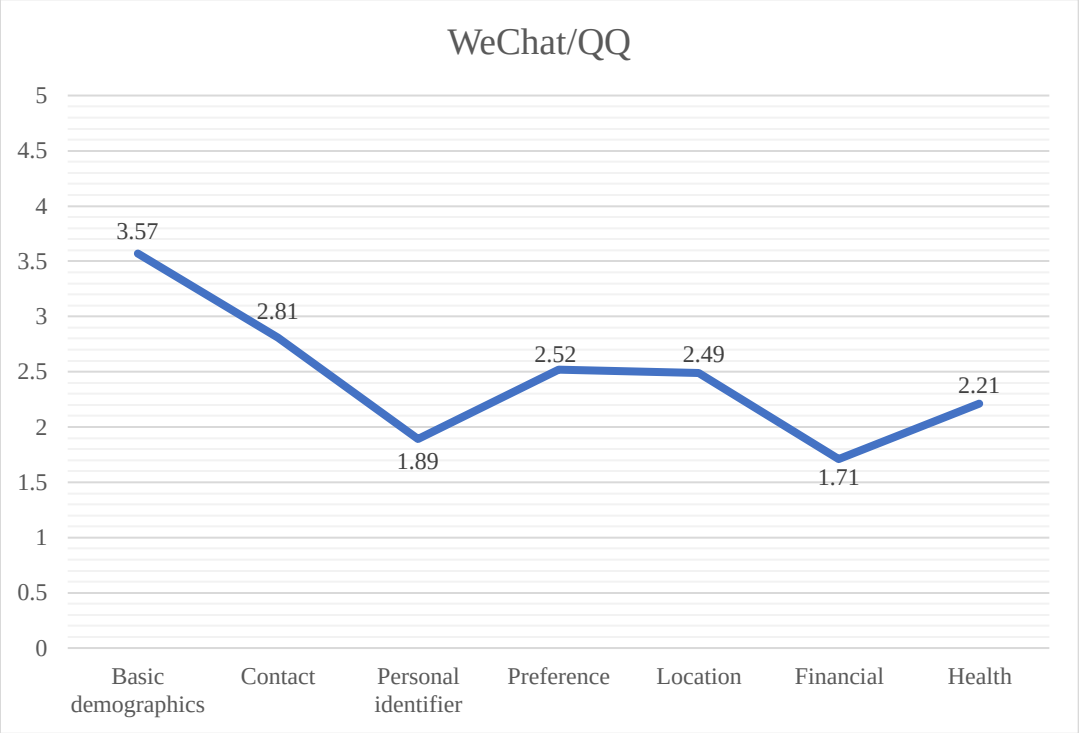

Figure 2 Willingness to Share Personal Information on Weibo

Figure 3. Willingness to Share Personal Information on Online Banking Platforms

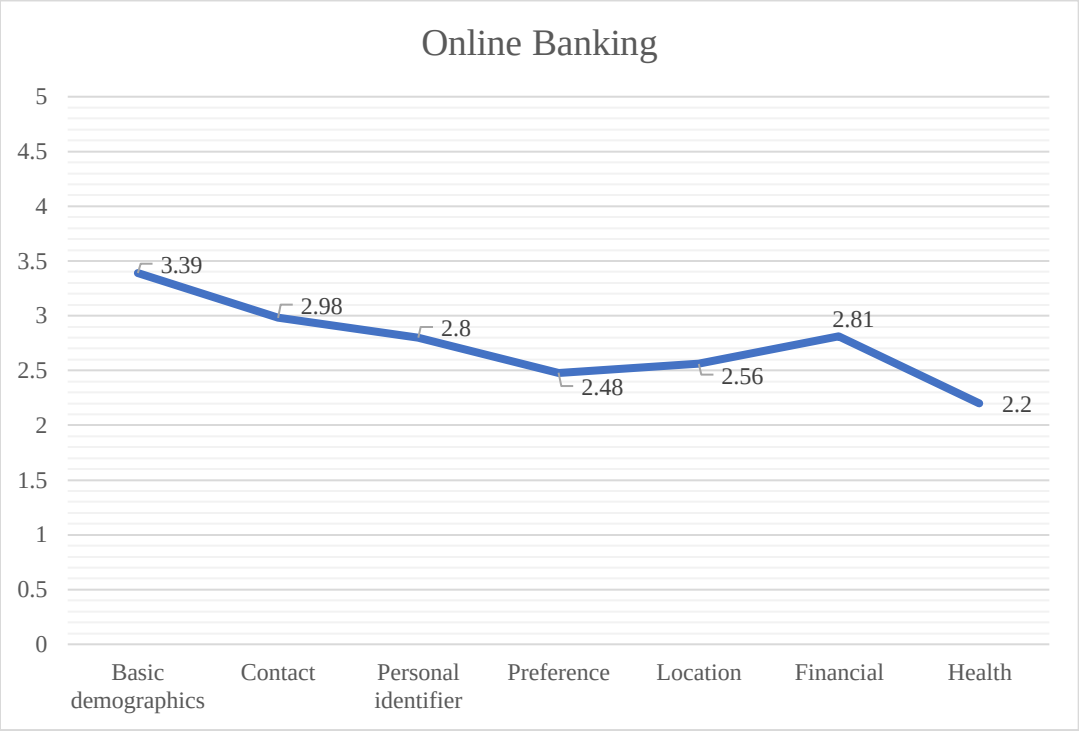

Figure 4. Willingness to Share Personal Information on Online Shopping Platforms

Figure 5. Willingness to Share Personal Information on Online Ridesharing Platforms

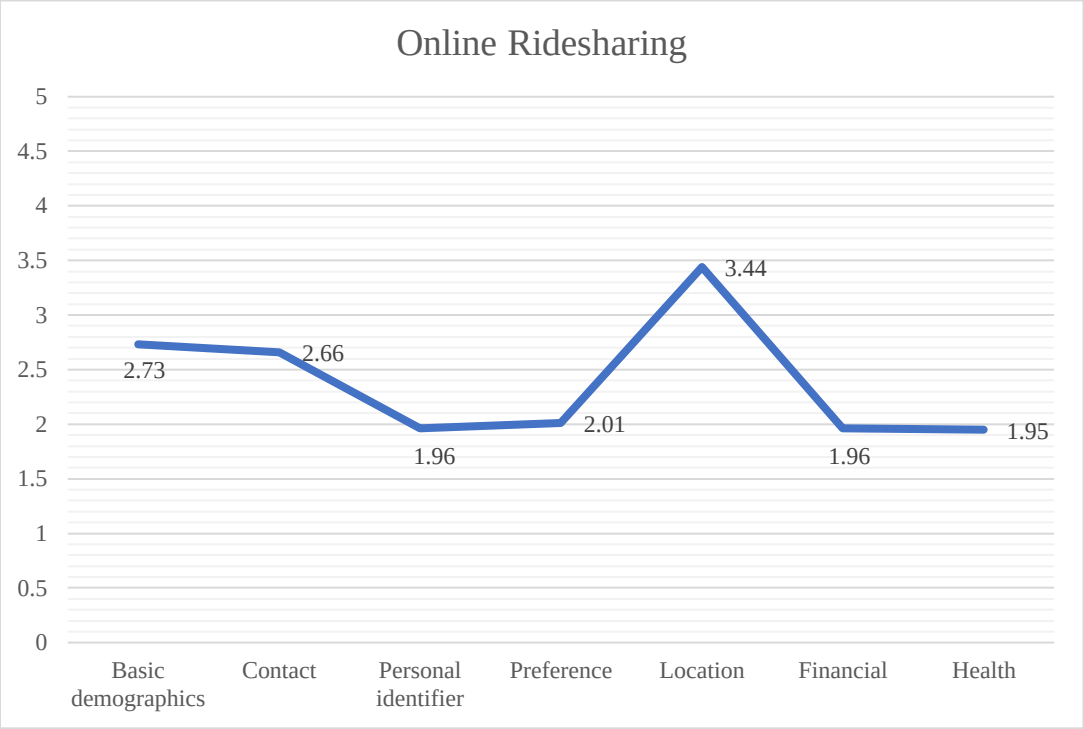

Figure 6. Willingness to Share Personal Information on Online Maps Platforms

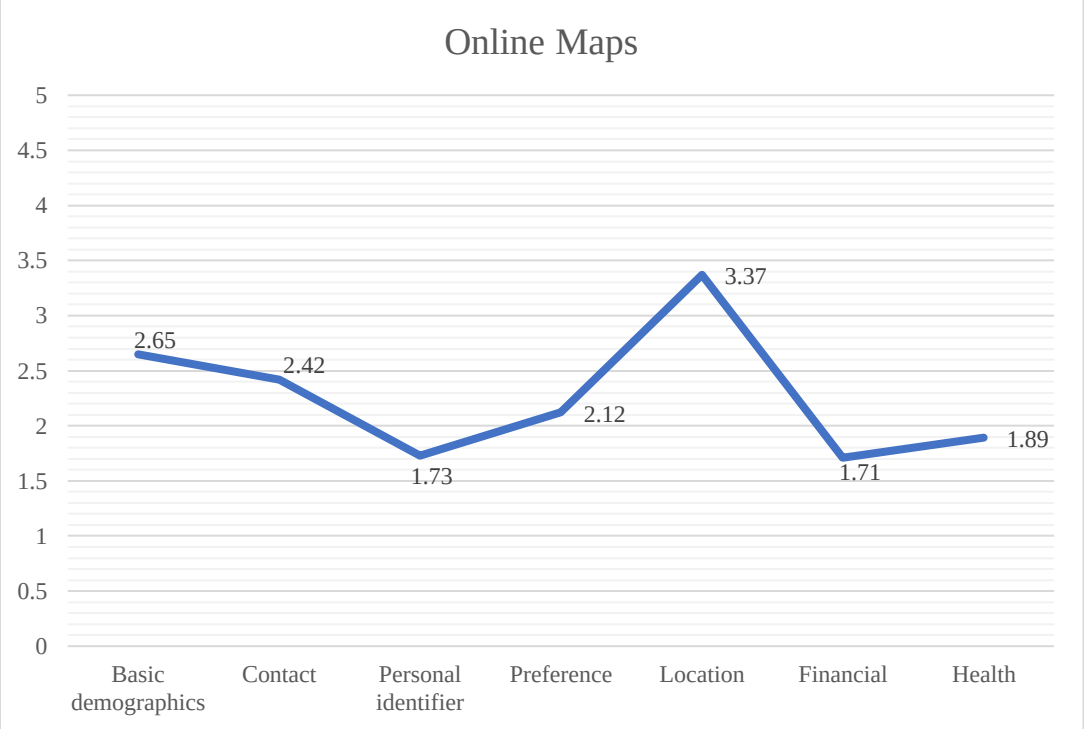

Figure 7. Willingness to Share Personal Information on Online Ticket Booking Platforms

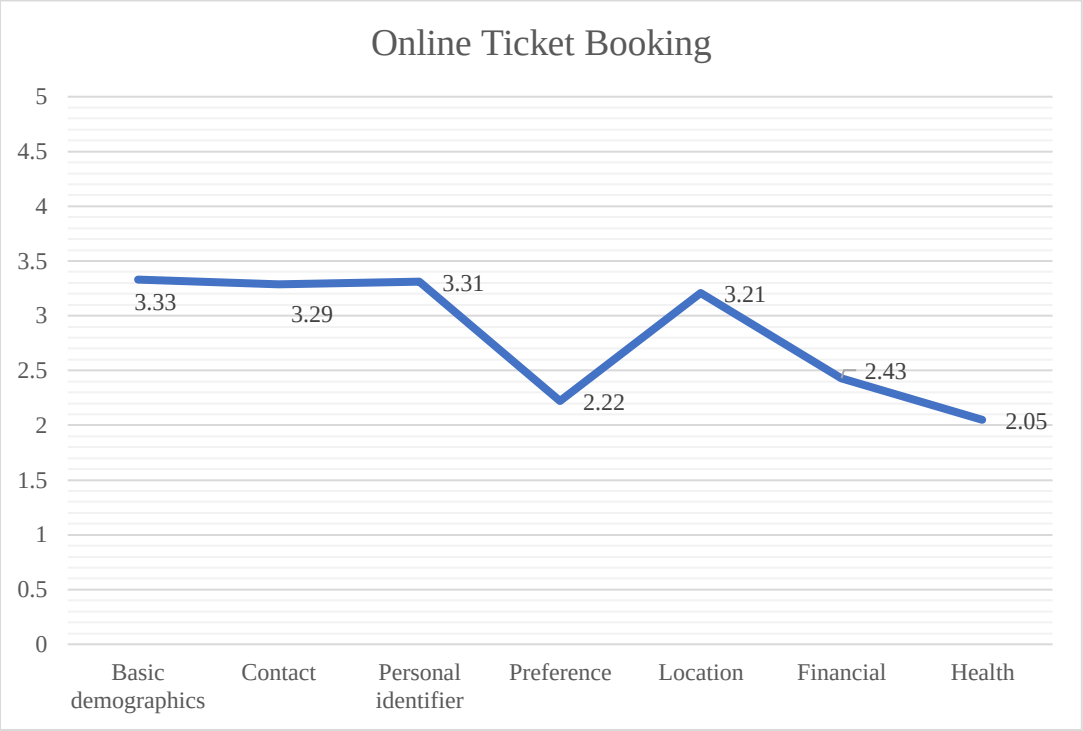

Figure 8. Willingness to Share Personal Information on Online Health Management Platforms

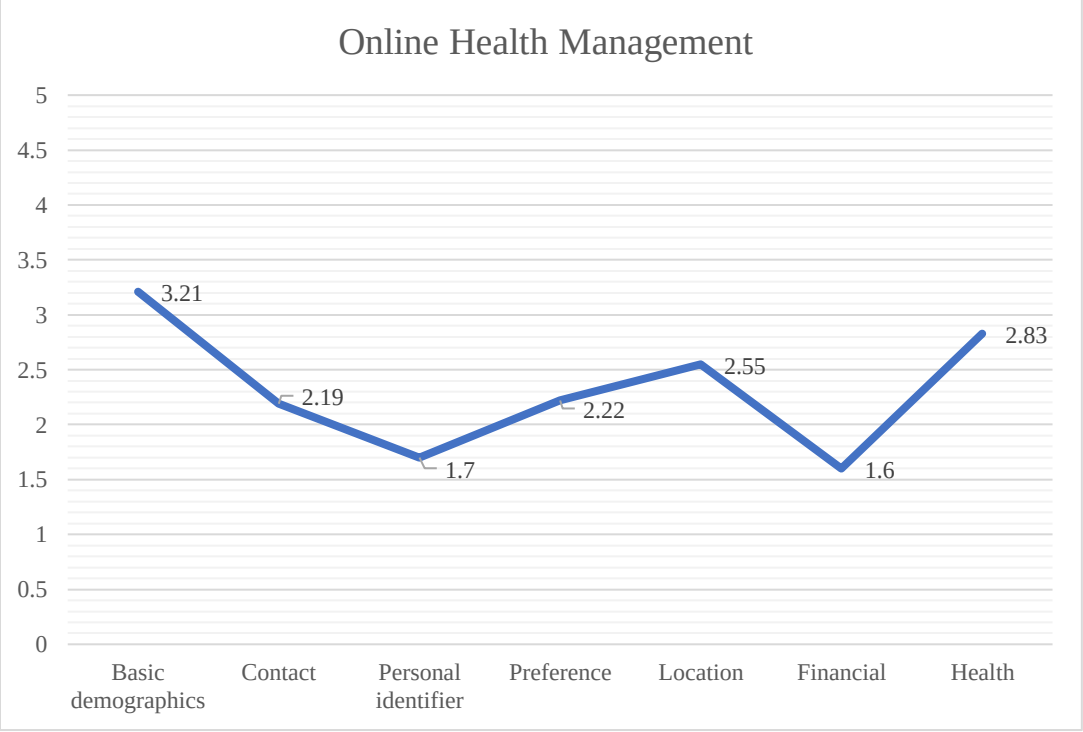

Figure 9. Privacy Efficacy Across Information Types

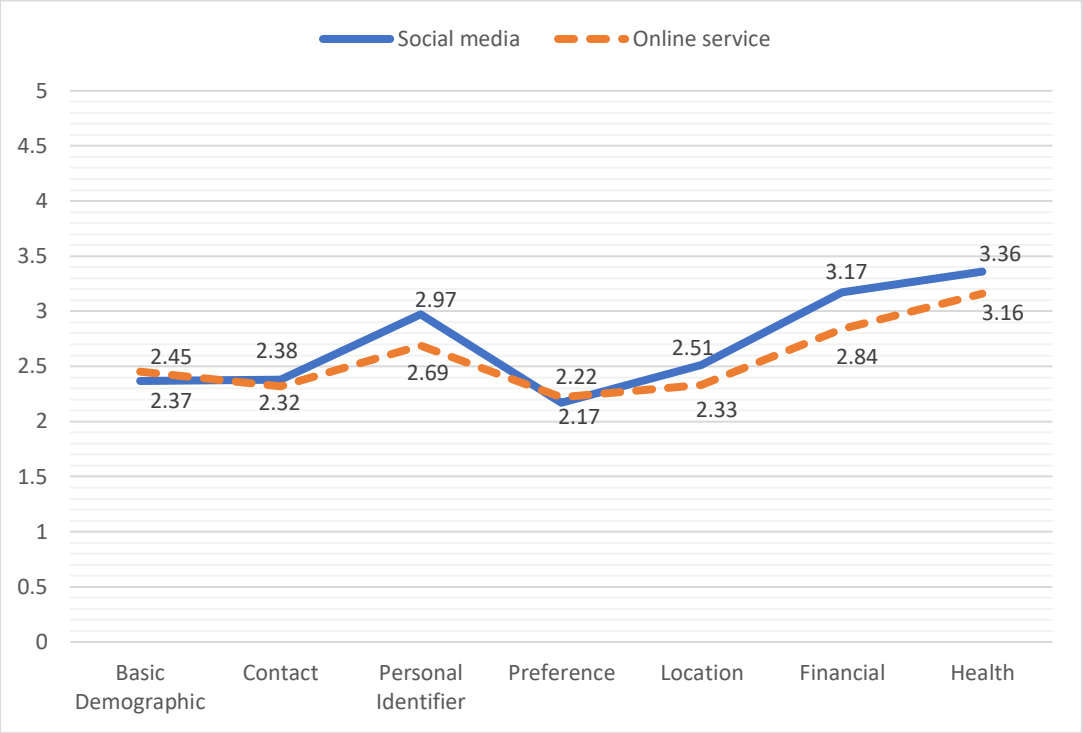

Table 8. Independent Sample t-test Result Comparing Web-based and Paper-based Responses on Key Variables

Variables	Survey mode				
	Web-based (*N*=728)		Paper-based (*N*=476)		
	M	*SD*	*M*	*SD*	*t*
Information privacy concerns	5.83	.65	5.79	.72	1.00
Government surveillance concerns	4.45	1.20	5.36	.97	-14.44**
Perceived need for government surveillance	4.95	1.10	4.55	1.17	6.01**
Willingness to disclose personal information	2.61	.50	2.32	.60	8.52**
Social media use	4.20	1.18	4.16	1.10	.59
Online service use	4.00	.81	4.02	.92	-.32
Adoption of protective strategies	3.78	.86	3.94	.82	-3.18**
Privacy efficacy	2.82	.66	2.37	.79	10.36**
Privacy literary	.68	.92	.84	1.25	-2.38*

** p<.001 * p<.05

APPENDIX 2: SURVEY QUESTIONNAIRE

Q1 It usually bothers me when online companies ask me for personal information.
Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q2 When online companies ask me for personal information, I sometimes think twice before providing it.
Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q3 It bothers me to give personal information to so many people.
Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q4 I am concerned that online companies are collecting too much personal information about me.
Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q5 Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q6 Consumer control of personal information lies at the heart of consumer privacy.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q7 I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q8 Online companies seeking information online should disclose the way the data are collected, processed, and used.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q9 A good consumer online privacy policy should have a clear and conspicuous disclosure.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q10 It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q11 I am concerned about the power the government has to wiretap Internet activities.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q12 I am concerned that my Internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q13 I am concerned about the government's ability to monitor Internet activities.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q14 The government needs to have greater access to personal information for efficiency and safety purposes.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q15 The government needs to have greater access to individual bank accounts for efficiency and safety purposes.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q16 The government needs broader wiretapping authority for security purpose.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q17 The government needs to have more authority to use high tech surveillance tools for Internet eavesdropping for security purpose.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q18 How much time have you spent per day using WeChat, QQ and Weibo over the past month?

	Less than 10 minutes	10 to 30 minutes	30 to 60 minutes	1 hour to less than 2 hours	2 hour to less than 3 hours	3 hour to less than 4 hours	More than 4 hours
WeChat	○	○	○	○	○	○	○
QQ	○	○	○	○	○	○	○
Weibo	○	○	○	○	○	○	○

Q19 How frequently have you used these online service over the past month?

	Never used it	Once	A few times	Once a week	A few times a week	Once a day	Several times a day
Online banking	○	○	○	○	○	○	○
Online shopping	○	○	○	○	○	○	○
Online ridesharing	○	○	○	○	○	○	○
Online mapping	○	○	○	○	○	○	○
Online ticket booking	○	○	○	○	○	○	○
Online health management	○	○	○	○	○	○	○

Q20 How frequently have you used per day using these online service over the past week?

	Less than 15 minutes	15 to 30 minutes	30 to 45 minutes	45 to 60 minutes	More than an hour
Online banking	○	○	○	○	○
Online shopping	○	○	○	○	○
Online ridesharing	○	○	○	○	○
Online mapping	○	○	○	○	○
Online ticket booking	○	○	○	○	○
Online health management	○	○	○	○	○

Q21 When using WeChat and QQ, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q22 When using Weibo, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q23 When using online banking services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q24 When using online shopping services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q25 When using online ridesharing services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q26 When using online mapping services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q27 When using online ticket booking services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q28 When using online health management services, to what extent are you willing to reveal the following personal information?

	Never willing	Slightly willing	Moderately willing	Very willing	Extremely willing
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q29 On a scale from 1 to 5, 1 being "no control at all", 5 being "a great deal of control", how much control do you think you have over these personal information when you use social media (WeChat, QQ, Weibo)?

	1	2	3	4	5
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Q30 On a scale from 1 to 5, 1 being "no control at all", 5 being "a great deal of control", how much control do you think you have over these personal information when you use online services (banking, shopping, ridesharing, mapping, ticket booking, health management)?

	1	2	3	4	5
Demographics (gender, age, education)	○	○	○	○	○
Contact information (email, phone number, address, social media accounts)	○	○	○	○	○
Personal identifiers (name, government ID)	○	○	○	○	○
Personal preference (browsing/keyword searching/shopping history)	○	○	○	○	○
Location (location history, real-time location)	○	○	○	○	○
Financial information (debit/credit card, financial status)	○	○	○	○	○
Health information (medical history, medical condition)	○	○	○	○	○

Think about the measures you usually take to protect your personal information when using social media and online service. Please indicate the extent to which you agree with each of the following statement.

Q31 I would consider making up fictitious responses to avoid giving websites real information about myself.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q32 I would resort to using another name or email address when registering with websites so I can have full access and benefits as a registered user without divulging my real identity.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q33 When registering with websites, I may only fill up data partially.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q34 I would like to make use of software so that the recipient cannot track the origin of my mail (e.g. re-mailers).

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Q35 I would use software to eliminate cookies that track my web-browsing behavior (e.g. JunkBuster, WRQ AtGuard)

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q36 I would like to make use of software to disguise my identity (e.g. Zero Knowledge, Anonymizer, Freedom).

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q37 I would refuse to provide personal information to this website/App.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q38 I would be reluctant to register with this website/App.

Strongly disagree
Disagree
Somewhat disagree
Neither agree nor disagree
Somewhat agree
Agree
Strongly agree

Q39 I would avoid using this website/App.

- Strongly disagree
- Disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Agree
- Strongly agree

Please indicate if the following statements about privacy policy are true.

Q41 If a website/APP has a privacy policy, it means that the website/APP cannot share information about you with other companies, unless you give the website your permission.

- True
- False
- I don't know

Q42 If a website/APP has a privacy policy, it means that the website/APP cannot give your address and purchase history to the government.

- True
- False
- I don't know

Q43 If a website/APP has a privacy policy, it means that the website/App must delete information it has about you, such as name and address, if you request them to do so.

- True
- False
- I don't know

Q44 If a website/APP violates its privacy policy, it means that you have the right to sue the website for violating it.

- True
- False
- I don't know

Q45 If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.

- True
- False
- I don't know

Q46 When you use the Internet to purchase products or to learn about medical conditions, advertisers are not allowed to track you in order to target advertisements.

- True
- False
- I don't know

We are toward the end of the this survey. Please answers these demographic questions.

Q47 You are

- Male
- Female
- Other
- Prefer not to answer

Q48 What is your major in college?

- Philosophy
- Economics
- Law
- Education
- Literature
- Media & Communication
- History
- Art
- Science
- Engineering
- Agronomy
- Medicine
- Management
- Other

Q49 What is your current age in years? Please enter the number in the box below.

Q50 What year are you in college?

- Freshmen
- Sophomore
- Junior
- Senior
- 5th grade
- Graduate student
- unclassified

This is the end of the survey. Thank you for your participation.

Survey Questionnaire in Chinese

信息社会个人数据保护调查问卷

您好！ 欢迎参与本次关于数据监视与个人信息保护的调查问卷。

本次问卷是一项学术研究，研究内容关于我们当下所处的信息社会的数据监视和个人信息保护，研究对象为在读本科生和研究生。您的参与可以帮助研究者进一步了解当下大学生使用社交媒体和服务类应用时的个人信息分享行为，以及当代大学生对个人信息隐私相关问题的理解和看法。本次问卷中，您将会被问及您对个人信息隐私和数据监视的关注、您的个人信息分享习惯、您对平台隐私政策的了解，以及您的社交媒体和服务类应用的使用习惯。本次问卷预计需要 10-15 分钟完成。

本次问卷允许参与者自主加入并匿名作答，参与者的身份信息不会在学术发表物中被直接或间接识别。本次研究数据将会被安全地保存在拥有高级密码保护的电脑中，除研究负责人之外不会有任何人接触到本次研究的数据。另外，本次问卷研究的目的限于推进普遍社会认知，您将不会因为参与本次问卷而获得特殊的个人利益。

如果您对本次问卷存在疑问，可以通过邮件 shaocy@live.unc.edu 联系该研究的负责人北卡罗来纳大学教堂山分校博士候选人邵成圆，您也可以通过电话+1(919)-966-3113 联系北卡罗来纳大学教堂山分校伦理审查委员会，该研究的伦理审查 ID 是 18-3180。

您必须是 18 周岁或以上，并且是在读本科生或研究生，才可以参与本次问卷研究。如果您满足以上条件并且愿意参与本次问卷，请在相应陈述前打钩表示同意参与。如果您不愿意参与，请将问卷交回发放人员。

☐ 我自愿参与本次研究，请开始问卷。

☐ 我不愿意参与本次研究，我会将问卷交回发放人

本次问卷第一部分问题是关于网络平台对用户个人信息的收集和使用，请选择您在多大程度上同意以下这些说法：

我不喜欢网络平台总是要我提供个人信息。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

当网络平台要求我提供个人信息时，我会三思而后行。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

把个人信息提供给很多不同的网络平台这让我很不安。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

我担心各种网络平台收集了过多的我的个人信息。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

用户的网络隐私问题就是用户能否掌控个人信息的收集、使用和共享的问题。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

用户对个人信息的掌控力是用户信息隐私的核心问题。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

我认为当用户对个人信息失去控制之时，或者当这种控制力被强制减少之时，用户的信息隐私已经被侵犯。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

网络平台在线获取用户个人信息时应该公开其数据收集、处理和使用途径。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

好的用户网络隐私政策应该有清晰、易懂的说明。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

了解我的个人信息被如何使用对我来说很重要。 (单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

以下问题关于政府公共机构在个人信息和网络安全方面的职能，请选择您在多大程度上同意以下这些说法：

政府公共机构监控网络活动的权力使我感到担忧。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

我担心我的账户和数据信息（例如邮件、购物记录、网页浏览记录等）将会越来越多地被公共和商业机构掌握。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

政府公共机构监视网络活动能力的增强使我感到担忧。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

政府公共机构需要拥有获取个人信息的能力，从而提高服务效率、保障网络安全。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

政府公共机构需要拥有获取个人银行账户信息的能力，从而提高服务效率、保障网络安全。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

政府公共机构需要拥有较大的监控网络安全的权力。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

政府公共机构应该使用先进的监视技术来保证网络安全。(单选题)

○ 坚决不同意 ○很不同意 ○有点不同意 ○无所谓同不同意 ○有点同意 ○很同意 ○坚决同意

接下来，请回想自己在过去一个月微信、QQ 和微博的使用情况，并回答以下问题：

在过去的一个月，您每天使用微博、QQ 和微信的时间大概是？(矩阵单选题)

	从不使用	30分钟以内	30分钟到1个小时	1个小时到2个小时	2个小时到3个小时	3个小时到4个小时	4个小时以上
微信	○	○	○	○	○	○	○
QQ	○	○	○	○	○	○	○
微博	○	○	○	○	○	○	○

请您回想自己在过去一个月**生活服务类应用**的使用情况，并回答以下问题：

在过去的一个月，您使用以下各种服务类应用的频率大概是？ (矩阵单选题)

	没使用过	用过一次	用过两三次	每周用一次	每周用三四次	每天用一次	每天用很多次
金融服务（网银、支付宝、微信支付等）	○	○	○	○	○	○	○
购物服务（淘宝、京东、美团等）	○	○	○	○	○	○	○
出行服务（滴滴出行、共享单车等）	○	○	○	○	○	○	○
实时地图（百度地图、高德地图等）	○	○	○	○	○	○	○
购票服务（携程、航班管家、12306 等）	○	○	○	○	○	○	○
健康管理（Keep、悦跑圈、大姨妈等）	○	○	○	○	○	○	○

下面请回想您在使用微信、QQ、微博和以上提到的 6 种服务类应用时需要提供的个人信息，并选择您在多大程度上愿意在使用这些服务时提供以下几类个人信息。这部分共有 9 个矩阵单选题，请您慢下来耐心回答。

使用**微信**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用 **QQ** 时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**微博**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**金融服务（网银、支付宝、微信支付等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○

身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**购物服务应用（淘宝、京东、美团等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**出行服务（滴滴出行、共享单车等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**地图服务（百度地图、高德地图等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**购票服务（携程、航班管家、12306 等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**健康管理（Keep、悦跑圈、大姨妈等）**时，您在多大程度上愿意提供以下几类个人信息？

	非常不愿意	不愿意	居中	愿意	非常愿意
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○

身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

下面请您考虑自己在使用社交媒体和服务类应用时对个人信息的掌控感，即自己在多大程度上能控制个人信息被收集、传播和再次使用，然后回答，如果 1 代表“没有任何掌控感”，5 代表“有很强的掌控感”，您认为有自己在多大程度上能控制个人信息的传播。 (矩阵单选题)

使用**社交媒体（微信、QQ、微博）**时，您感觉自己在多大程度上能控制以下几类个人信息不被抓取和使用？

	1	2	3	4	5
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

使用**生活服务类应用**（以上所提到的金融、购物、出行、地图、购票、健康管理等类别）时，您感觉自己在多大程度上能控制以下几类个人信息不被抓取和使用？

	1	2	3	4	5
人口统计类信息（性别、年龄、教育程度）	○	○	○	○	○
联系信息（邮件、电话、地址、微信/QQ）	○	○	○	○	○
身份信息（姓名、身份证号）	○	○	○	○	○
个人偏好（网页浏览/搜索/购物历史）	○	○	○	○	○
所在位置（位置历史、实时位置）	○	○	○	○	○
金融信息（信用/储蓄卡号、支付宝账号）	○	○	○	○	○
健康信息（疾病历史、健康现状）	○	○	○	○	○

接下来，请您考虑平时使用社交媒体和服务应用时如何保护个人信息，并选择以下保护个人信息的说法在多大程度上符合您的做法：

我会填写虚构的身份信息，从而避免提供真实的个人信息。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会使用别名和不常用的邮箱地址来注册，这样我就可以在不提供真实个人信息的情况下使用该服务(单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我注册的时候可能只填写一小部分个人信息。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会使用具有删除网页浏览历史和删除 Cookies 功能浏览器。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会使用随机密码生成软件（比如 One Password, Last Pass），来保护个人信息数据安全。

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会使用具有隐藏或更改自己 IP 地址的服务（比如 VPN）来保护我的个人信息不被轻易追踪 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会选择不注册需要提供个人信息的网站或服务应用。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会拒绝向网站或服务应用提供个人信息。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

我会不再访问提供过个人信息的网站或服务应用。 (单选题)

○ 极其不符合 ○很不符合 ○有点不符合 ○无所谓符不符合 ○有点符合 ○很符合 ○极其符合

了解网络平台的隐私政策对保护个人信息至关重要。请您判断以下关于平台隐私政策的说法是正确、错误，还是您也不太清楚：

如果一个网络平台有隐私政策，这意味着，除非得到您的同意，该网络平台不能与其它公司分享你的个人信息。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

如果一个网络平台有隐私政策，这意味着它不能把你的地址和购物点击记录交给政府机构。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

如果一个网络平台有隐私政策，这意味着只要你提出要求，它就必须删除你的个人信息，比如姓名和地址。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

如果一个网络平台违反了它的隐私政策，你可以以此为由起诉这个平台。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

网络平台追踪你的网站的浏览记录必须经过你的同意。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

当你使用网络服务购买产品或者咨询疾病时，广告商不能追踪你的浏览历史并以此为根据投放针对性广告。 (单选题)

○ 正确　　○ 错误　　○ 我不太清楚

本次问卷即将结束，最后请您提供以下几项匿名信息：

您是 (单选题)

○ 男生
○ 女生
○ 不方便回答

您的专业是？如果您是双学位，请选择主修学位。 (单选题)

○ 哲学　○ 法学　○ 教育学　○ 文学　○ 新闻与传播学　○ 历史学　○ 艺术

○ 理学　○ 工学　○ 农学　○ 医学　○ 管理学　○ 其它

您的年龄是？ (填空题)

您现在读大学几年级？ (单选题)

- ○ 大一
- ○ 大二
- ○ 大三
- ○ 大四
- ○ 大五
- ○ 研究生（硕士、博士）

本次问卷到此结束，感谢您的耐心填写！

REFERENCES

Aas, K.F., H.O. Gundhus, and H.M. Lomel. 2008. *Technologies of Insecurity: The Surveillance of Everyday Life*. London: Routledge

Abrams v. United States, 250 U.S. 616.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497.

Baker, C. E. (1992). *Human liberty and freedom of speech*. Oxford University Press on Demand.

Baker, C. E. (2010). Autonomy and Free Speech. *Const. Comment.*, *27*, 251-282.

Baker, R., et. al. (2013). Report of the AAPOR task force on non-probability sampling. Retrieved from http://www.aapor.org/AAPOR_Main/media/MainSiteFiles/NPS_TF_Report_Final_7_revised_FNL_6_22_13.pdf

Balkin, J. M. (2014). Old school/new school speech regulation. *Harvard Law Review*, *127*,

Bamman, D., O'Connor, B. & Smith, N. A. (2012). Censorship and deletion practices in Chinese social media, *First Monday*, *17* (3), Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3943/3169

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Barnes, S. B. (2006). A privacy paradox: Social networking in the Unites States. *First Monday, 11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.

Baxter, L. A., & Babbie, E. R. (2004). *The basics of communication research*. Cengage Learning.

Bunker, M. D. (1996). First amendment theory and conceptions of the self. *Communication Law and Policy, 1*(2), 241-269.

Bennett, C. J. (2011). In defence of privacy: The concept and the regime. *Surveillance & Society*, *8*(4), 485-496.

Bol, P. K. (1993). Government, Society, and State: On the Political Visions of Ssu-ma Kuang (1019-1086) and Wang An-shih (1021-1086). In: Hymes, R. & Schirokauer, C. *Ordering the World: Approaches to State and Society in Sung Dynasty China*. Berkeley: University of California Press.

Botsman, R. (2017, Oct 21). Big data meets Big Brother as China moves to rate its citizens. *WIRED*. Retrieved from https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Bunker, M. D. (2001). *Critiquing free speech: First Amendment theory and the challenge of interdisciplinarity*. Routledge.

Carney, M. (2018, Sept 17). Leave no dark corner. *ABC News*, Retrieved from https://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197889940=1Cohen, J. E. (2008). Privacy, Visibility, Transparency, and Exposure. *The University of Chicago Law Review*, *75*(1), 181–201.

Chang, L., & Krosnick, J. A. (2009). National Surveys Via Rdd Telephone Interviewing Versus the InternetComparing Sample Representativeness and Response Quality. *Public Opinion Quarterly*, *73*(4), 641–678. https://doi.org/10.1093/poq/nfp075

Chase, M. & Mulvenon J. (2002). *You've got dissent: Chinese dissident use of the Internet and Beijing's counter-strategies*. Santa Moica, CA: Rand.

Cheung, A. S. Y. (2009). China Internet going wild: Cyber-hunting versus privacy protection. *Computer Law & Security Review*, *25*(3), 275–279. https://doi.org/10.1016/j.clsr.2009.03.007

China Internet Network Information Center (2018*). The 42nd statistical report on Internet development in China*, January, 2018. Accessed online at https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf

Chinese Ministry of Education (2017). List of Higher Education Institutes. Retrieved from http://www.moe.gov.cn/srcsite/A03/moe_634/201706/t20170614_306900.html

Chinese Ministry of Education (2018). *Number of Students in Higher Education Institutions.* Retrieved from http://www.moe.gov.cn/s78/A03/moe_560/jytjsj_2017/qg/201808/t20180808_344685.html

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, *127*, 1904-1933.

Cohen, J. (2015). Studying Law Studying Surveillance. *Surveillance & Society*, *13*(1), 91–101. https://doi.org/10.24908/ss.v13i1.5160

Cooke, M., Watkins, N., & Moy, C. (2009). A Hybrid Online and Offline Approach to Market Measurement Studies. *International Journal of Market Research*, *51*(1), 29–48. https://doi.org/10.2501/S1470785308200298

Deleuze, G. & Guattari, F. (1987). *A Thousand Plateaus*. Minneapolis: University of Minnesota Press.

Deutskens, E., de Jong, A., de Ruyter, K., & Wetzels, M. (2006). Comparing the generalizability of online and mail surveys in cross-national service quality research. *Marketing Letters, 17*(2), 119–136. https://doi.org/10.1007/s11002-006-4950-8

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83–108.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation 144. *The Journal of Strategic Information Systems, 17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors: The relation between privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail and Mixed-Mode Surveys: The Tailored Design Method.* Wiley.

Doffman, Z. (2019, May 3). China is using facial recognition to track ethnic minorities, even in beijing. *Forbes.* https://www.forbes.com/sites/zakdoffman/2019/05/03/china-new-data-breach-exposes-facial-recognition-and-ethnicity-tracking-in-beijing/#707b65e734a7

Dworkin, G. (1988). *The theory and practice of autonomy*. Cambridge University Press.

European Parliament and Council (1995, Oct 24). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195–219. https://doi.org/10.1108/10662240510590360

The Financial (2015). China business analytics services market undergo accelerated growth including Big Data deployments. Retrieved from https://www.finchannel.com/technology/44166-china-business-analytics-services-market-undergo-accelerated-growth-including-big-data-deployments

Fish, S. (1994). *There's no such thing as free speech: And it's a good thing, too*. Oxford University Press.

Foucault, M. (2012). *Discipline and punish: The birth of the prison*. Vintage.

Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972-1977*. Pantheon.

Gaouette, N, Labott, E, Griffith, J. & Westcott, B. (2018, Oct 4). Pence attacks China on "predatory" trade, "coercion" and military "aggression." CNN, Retrived from https://www.cnn.com/2018/10/04/politics/pence-china-trump-intl/index.html

Gilliom, J., & Monahan, T. (2012). *SuperVision: An introduction to the surveillance society*. University of Chicago Press.

Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

Goldsmith, J., & Wu, T. (2006). Who controls the Internet?: illusions of a borderless world. Oxford University Press.

Greenhalgh, S, & Edwin A. W. (2005). *Governing China's Population: From Leninist to Neoliberal Biopolitics*. Stanford: Stanford University Press.

Haggerty, D., Richard, V., & Ericson, K. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Higher Education Evaluation Center (2017, Oct. 16). How far are we from the best undergraduate education? *People.com*. Retrieved from http://edu.people.com.cn/n1/2017/1016/c367001-29588492.html

Hoofnagle, C. J., & Urban, J. (2014). Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review*, *49*, 216–317.

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. *Surveillance & Society*, *15*(3/4), 418–424.

Hughes, C. R. (2003). Review Essay: China and the Internet: A Question of Politics or Management? *The China Quarterly*, *175*, 828-824. Retrieved from https://doi.org/10.1017/S0305741003000468

Jeffereys, E & Sigley, G. (2009). Governmentality, governance, and China. in Jeffreys, E. (Ed.). *China's governmentalities: governing change, changing government*. Routledge.

Jiang, M. (2010). Authoritarian informationalism: China's approach to Internet sovereignty. *SAIS Review of International Affairs*, *30*(2), 71–89.

Kant, I. (1784). What is enlightenment. Retrieved from http://www.columbia.edu/acis/ets/CCREAD/etscc/kant.html

Kemper, E. A., Stringfield, S. & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. In Tashakkori, A. Teddlie, C. & Teddlie, B (Ed.). *Handbook of mixed method in social and behavioral research*. SAGE.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326-343.

Kuo, F.-Y., Lin, C. S., & Hsu, M.-H. (2007). Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices. *Journal of Business Ethics*, *73*(2), 145–160. https://doi.org/10.1007/s10551-006-9179-1

Lavrakas, P. J. (2008). *Encyclopedia of survey research methods*. Thousand Oaks, CA: Sage Publications, Inc.

Lee, J. A., Liu, C. Y. & Li W. P (2013). Searching for Internet freedom in China: A case study on Google's China experience, *Cardozo Arts & Entertainment Law Journal,31,* 405-434.

Lee, J. A. & Liu C. Y. (2016). Real-name registration rules and the fading digital anonymity in China, *Washington International Law Journal, 25*, 1-34.

Lemke, T. (2011). *Foucault, governmentality, and critique*. Paradigm Publishers.

Leibold, J. (2011). Blogging alone: China, the internet, and the democratic illusion?. *The Journal of Asian Studies*, *70*(4), 1023-1041.

Lensvelt-Mulders, G. J., Lugtig, P. J., & Hubregtse, M. (2009). Separating Selection Bias and Non-coverage in Internet Panels using Propensity Matching.

Luther, C. A. (2011). Survey. In S. Zhou, S. & Sloan, W. D. (Eds.), *Research methods in communication* (5th ed.) (p. 145-160). Northport, AL: Vision Press.

Lyon, D. (1994). *The electronic eye: The rise of the surveillance society*. Minneapolis: University of Minnesota Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education (UK).

Lyon, D. (2002). Surveillance Studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society, 1*(1), 1–7.

Lyon, Ball & Haggerty (2012). *Routledge Handbook of Surveillance Studies*. Routledge.

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society, 13*(2), 139–152.

Mac R. , Adams, R. & Rajagopalan, M. (2019, June 5). US universities and retirees are funding the technology behind China's surveillance state. BuzzFeed News.

https://www.buzzfeednews.com/article/ryanmac/us-money-funding-facial-recognition-sensetime-megvii

MacKinnon, R. (2009). "China's censorship 2.0: How companies censor bloggers." *First Monday* 14(2). Available at http://firstmonday.org/article/view/2378/2089.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science & Technology Law Review*, *18*, 176-218.

Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393.

Meiklejohn, A. (1961). The First Amendment is an absolute. *The Supreme Court Review*, *1961*, 245-266.

Mei, B., & Brown, G. T. L. (2017). Conducting Online Surveys in China. *Social Science Computer Review*, 1-14. https://doi.org/10.1177/0894439317729340

Meiklejohn, A. (2000). *Free speech and its relation to self-government*. The Lawbook Exchange, Ltd.

McDougall B. S. & Hansson A. (Eds.) (2002). *Chinese concepts of privacy*. Leiden, The Netherlands: Koninklijke Brill NV.

Mitchell, A. & Diamond, L. (2018, Feb 2). China's Surveillance State Should Scare Everyone. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

Milton, J. (1868). *Areopagitica: 1644*. Alex. Murray.

Mill, J. S. (1966). On liberty. In *A selection of his works* (pp. 1-147). Palgrave, London.

Millward, J. A. (2018, Feb 3). What it's like to live in a surveillance state. *The New York Times*. Retreived from https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html

Moy, P., & Murphy, J. (2016). Problems and prospects in survey research. *Journalism & Mass Communication Quarterly*, *93*(1), 16–37.

Mozur, P. (2019, April 14). One month, 500,000 face scans: How China is using A.I. to profile a minority. *The New York Times*. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law*, *20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*, 215–236.

Pasek, J. (2016). When will Nonprobability Surveys Mirror Probability Surveys? Considering Types of Inference and Weighting Strategies as Criteria for Correspondence. *International Journal of Public Opinion Research*, *28*(2), 269–291. https://doi.org/10.1093/ijpor/edv016

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Price, P. C., Jhangiani,R. & Chiang, I. A. (2015). *Research methods in psychology*, 2nd Canadian Edition. Creative Commons Attribution NonCommercial ShareAlike. https://opentextbc.ca/researchmethods/

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*, *126*, 1934-1965.

Rule, J. B. (2007). *Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience*. Oxford University Press.

Shen, Q. (2015). Liyi, fengxian yu wangluoxinxi yinsi renzhi: Yi Shanghai daxuesheng wei yanjiu duixiang [Benefits, risk, and perceptions of Internet information privacy: a study of college student in Shanghai], Chinese Journal of Journalism & Communication, 7, 85-100.

Shen, Q. (2017). Fengxian yu chengben de quanheng: Shejiao wangluo zhong de "Yinsi Beilun" [Balancing risk against benefits: the "Privacy Paradox" on social media], *Journalism & Communication*, *8*, 55-69.

Sills, S. J., & Song, C. (2002). Innovations in survey research: An application of web-based surveys. *Social Science Computer Review*, *20*(1), 22–30.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Solove, D. J. (2013). Introduction: Privacy Self-Management and Consent Dilemma. *Harvard Law Review*, *126*, 1880-1903.

Solove, D. J. (2015). The legacy of Privacy and Freedom, in Westin, A. F. (2015). *Privacy and Freedom*. Ig Publishing.

Staples, W. G. (2014). *Everyday surveillance: vigilance and visibility in postmodern life.* Lanham, Md.: Rowman & Littlefield Publishers.

Statista (2018). Internet usage worldwide. Retrieved from https://www.statista.com/study/12322/global-internet-usage-statista-dossier/

Shiffrin, S. H. (2016). *What's Wrong with the First Amendment*. Cambridge University Press.

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust insights from a national survey. *New Media & Society*, *9*(2), 300–318.

Vuori, J. A., & Paltemaa, L. (2015). The lexicon of fear: Chinese internet control practice in Sina Weibo microblog censorship. *Surveillance & Society*, *13*(3/4), 400–421.

Wang, H. (2011). *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*. Springer Berlin Heidelberg.

Wang L. (2012). Yinsiquan gainian de zaijieding [Calibrating the concept of privacy], *The Legal Scholar*, 1(1), 108-120.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Watt, J. H, & Berg, S. V. D. (2002). *Research methods for communication science*. Accessible online at http://www.cios.org/readbook/rmcs/rmcs.htm

Westin, A. F. (2015). *Privacy and Freedom*. Ig Publishing.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453.

Whitman, C. B. (1985). Privacy in Confucian and Taoist thought. In Munro, D. & Arbor, A.(Eds), *Individualism and Holism: Studies in Confucian and Taoist Values* (pp. 85–100). University of Michigan Center for Chinese Studies.

Wright, K. B. (2005). Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and

Web Survey Services. *Journal of Computer-Mediated Communication*, *10*(3). https://doi.org/10.1111/j.1083-6101.2005.tb00259.x

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy*, *35*(7), 603–616. https://doi.org/10.1016/j.telpol.2011.05.002

Wutongguo (2018). *Blue book on campus recruitment in China* (Fall 2018). Beijing, China Book Press.

Xue, H. (2010). Privacy and personal data protection in China: An update for the year end 2009. *Computer Law & Security Review*, *26*(3), 284–289. https://doi.org/10.1016/j.clsr.2010.01.004

Yao-Huai, L. (2005). Privacy and Data Privacy Issues in Contemporary China. *Ethics and Information Technology*, *7*(1), 7–15. https://doi.org/10.1007/s10676-005-0456-y

Yang, G. (2014). Political contestation in Chinese digital spaces: Deepening the critical inquiry. *China Information*, *28*(2), 135–144.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

Zarrow P. (2002). The origins of modern Chinese concepts of privacy: Notes on social structure and moral discourse, in McDougall B. S. & Hansson A. (Eds.) *Chinese concepts of privacy*, p. 121-146. Leiden, The Netherlands: Koninklijke Brill NV.

Zhang Xinbao (2004). *Yinsiquan de falv baohu [The legal protections of privacy]*. Qunzhong Publication.

Zhu, G. (1997). The right to privacy: An emerging right in Chinese law, *Statute Law Review*, *18*(3), 208-214.